International Journal of Advanced Science and Technology
Vol.111 (2018), pp.11-22
http://dx.doi.org/10.14257/ijast.2018.111.02

A Comprehensive Review of Mitigation Techniques for Blackhole Attack in AODV Routing Protocol in MANETs

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 is a self-configuring network that has no infrastructure and communication happens in multi-hop fashion. This dynamic nature of MANET and lack of infrastructure makes it prone to many types of routing and security attacks. Ad-hoc On-demand Distance Vector is the most commonly preferred routing protocol in which route is formulated only when it is needed in a reactive manner. AODV is prone to a kind of packet drop attack called blackhole attack. In this paper, we have reviewed many existing solutions that are useful in mitigation of blackhole attack. These mechanisms are categorized as detection and prevention methodologies in the review. We have provided a detail on these mechanisms involving the concept of mechanism, simulation and result in brief and critically review them for their drawbacks and advantages along with their simulation and result highlights. A comparison is drawn and finally, the future research areas are identified on which the research should focus.

Keywords*: Mobile Ad-hoc Networks, Blackhole Attack, Grayhole Attack, Ad-hoc On-demand Distance Vector Routing Protocol, Trust Algorithm*

1. Introduction

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

Received (December 30, 2017), Review Result (February 5, 2018), Accepted (February 11, 2017)

ISSN: 2005-4238 IJAST

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

2. AODV Routing Protocol

AODV [5] is an acronym for Ad-hoc On-demand Distance Vector Routing protocol that establishes a connection between two nodes whenever needed. This protocol works in re-active manner and all the nodes maintain a routing table in their respective memory that will give the information about the next hop to a particular destination node, hop count and some other relative information. Three control packets are used for route maintenance and establishment. These three packets are RREQ, RREP and RERR packets. RREQ (Route REQuest) packet is sent by any MANET node implementing AODV routing protocol whenever it needs to find route to a particular destination.

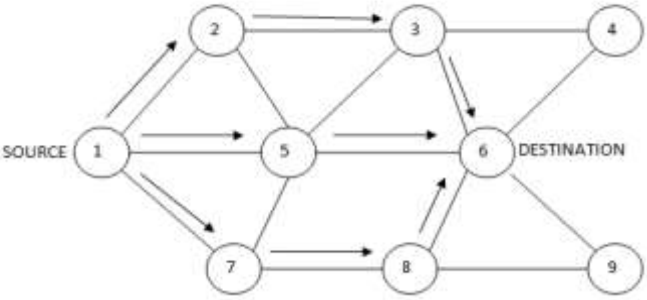

Figure 1. Source Node Sending RREQ Packet

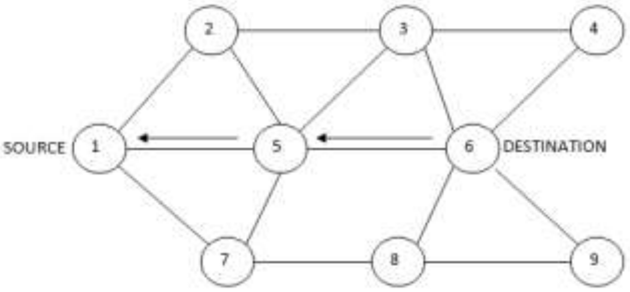

Figure 2. Node Sending RREP Packet

The node first checks its routing table and if the routing information is available then it uses that information for sending the data packet. If there is no entry in the routing table about that particular destination with which the node wants to communicate, then it broadcasts RREQ packet to all its neighbouring nodes. After receiving a RREQ packet, each node checks its routing table for entry for the destination for which the RREQ packet has broadcasted. If it has the route to that destination, then that node replies with a RREP (Route REPly) packet, otherwise it further broadcasts the same RREQ packet to its neighbourhood. The RREP packet is unicasted back to the originator of the respective RREQ packet. Using this RREP packet, all the intermediate nodes up to source node updates their routing table for that particular destination accordingly. The RERR (Route ERRor) packet is used by any intermediate node to notify the source about disruption of path to the particular destination. The RERR packet is also unicasted towards the source node of the data packet. RERR packet, on the contrary, is used during the actual data transmission and not in the route discovery.

The structure of these three packets used in AODV route establishment and maintenance is described as below:-

0 31
Source IP Address
Source Sequence No.
Broadcast-ID
Destination IP Address
Destination Sequence No.
Hop Count
Other Required Information (Variable and Implementation Dependent)

Figure 3. Structure of RREQ Packet

0 31
Destination IP Address
Source IP Address
Broadcast-ID
Destination Sequence No.
Source Sequence No.
Hop Count
Lifetime
Other Required Information (Variable and Implementation Dependent)

Figure 4. Structure of RREP Packet

0 31
Destination IP Address
Source IP Address
Broadcast-ID
Destination Sequence No.
Source Sequence No.
Hop Count
Reason for Link Failure
Other Required Information (Variable and Implementation Dependent)

Figure 5. Structure of RERR Packet

In AODV implemented network, each node maintains two monotonically increasing counters known as broadcast-id and sequence number. These numbers are incremented every time when the node issues a route discovery process for a particular destination node. AODV routing protocol uses broadcast ID and source IP address as prime attributes to identify a particular RREQ packet uniquely in the network. The broadcast-id will remain the same for a single RREQ packet generated by the source node. Apart from these some other information like destination IP address, destination sequence number, hop count, *etc* are some other fields used in RREQ packet that serves various purposes. Destination sequence number field provides the last known sequence number by the source node for that particular destination and an intermediate node will only send back a RREP packet if it has an entry in routing table for that destination with destination sequence number greater than provided in this field. Whenever any node receives RREQ packet, it checks for the destination IP address and refers its own routing table for that IP address. If an entry exists for that node, it checks for the sequence number. If the sequence is in accordance to the criteria of the protocol, then it will reply with RREP packet unicasted back to the previous hop from which it receives that RREQ packet and so on. With flooding of RREQ packet, a node is bound to receive same RREQ packet from multiple other neighbouring nodes. So, each node checks the broadcast-id of RREQ packet and if it has already processed the RREQ packet and forwards it further or unicasts [17] RREP packet, it will ignore that RREQ packet.

3. Blackhole Attack

Blackhole attack is a very destructive packet drop attack in which the malicious node on receiving a RREQ packet replies with a fake RREP packet that contains small hop count and a destination sequence number that makes the source believes that RREP packet sent by attacking node is genuine and that node really has the most optimal path to that particular destination even though that attacking node has no route to that destination. When the source node actually transmits a data packet to that Blackhole node, the blackhole node drops that packet and does not forward it further.

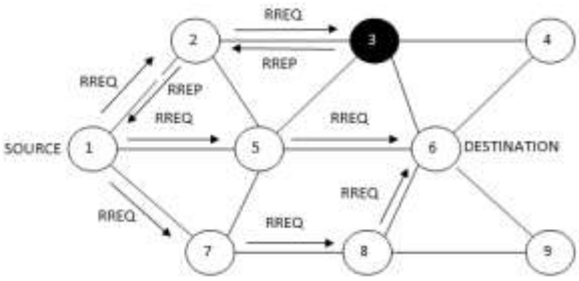

Figure 6. Blackhole Node Sending Fake RREP Packet to Source

In the figure, the scenario of Blackhole attack is illustrated. In the above illustration, node 3 is the attacking node, node 1 is the originator of RREQ packet and it initiates a route discovery mechanism to establish a path to the destination node 6. Node 3, which is a Blackhole node, on receiving the RREQ packet generates fake RREP packet with relatively smaller hop count and destination sequence number that is a little higher than the destination sequence number placed in the field of RREQ packet last known to the source. On receiving the RREP packet generated by node 3, the source node 1 got assured that this path is the optimal one. But, when node 1, sends a data packet to the destination node 6, then node 3 on receiving the data packet drops it and does not forward it any further.

The blackhole attack drastically drops the packet delivery ratio and if no counter measure is taken against this attack, it can almost shut down the communication in virtually any network. However, using counter measures will help in mitigating Blackholes to quite some extent. So, normally blackhole attacking node do not drops all the packets but act selectively to drop only some packets while forwarding some of the packets. In this way it may prevent detection through counter measures that are not that sound. This form of Blackhole attack is called Grayhole attack.

4. Counter-measures for Blackhole Attack

There are several mechanisms developed by researchers for mitigation of Blackhole attacks in MANET and we have comprehensively reviewed 48 research papers published since 2012 in esteemed and reputed journals. Out of these, we have briefly reviewed research mechanisms of 9 research papers that provide a comprehensive overview of research in past five years. The mitigation of Blackhole attack is done through two differently followed methodologies; one is detection of source of attack and the other is prevention of attack. In detection mechanism, mechanism is devised in such a way that helps in detection of Blackhole attacks either pro-actively or in re-active manner. On the other hand, in prevention mechanism, the prime objective is to avoid any blackhole to participate in path establishment process. But if a Blackhole somehow manage to get into the route establishment identifying and marking that malicious node is also done in the prevention mechanism, although this is secondary objective of mechanism. Some of the important counter-measures for mitigation of 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**
Collaborative Bayesian Watchdog [18]	NS-2	Detection	Bayesian filter and collaboration among nodes	Detection rate is 97%	Extensive overhead due to co-operation in detection
CUSUM [19]	NS-3	Detection	Sequence Number based approach	Detection rate lies in the range of 95-98%	Computational overheads, high order hardware capabilities requirement
MBDP-AODV [20]	NS-2.35	Prevention	Statistical metrics for sequence number	PDR is increased to 92%	Cannot detect smartly executed Grayhole attack, overheads due to alert packets
Trust and Energy Based algorithm [21]	NS-2	Prevention	Trust Algorithms	PDR is increased to 75%	Averaging the trust provides a loop hole for smart Grayhole attack
Distributed	NS-2	Preventio	Statistical	PDR is	Network

Co-Operative Approach [22]		n	analysis of communication parameters	increased to 93%	overhead, no dissemination of Blackhole information after detection
Opinion Based Trust Based Scheme [23]	NS-2.35	Detection	Co-operative trust based approach	Detection rate is approximately 96%	Opinions cause high level overhead, network is prone to attacks in its initial phase
CORIDS [24]	Qualnet	Detection	Cluster head as IDS	Shows 97% detection rate in Blackhole attack	Use of CH requires high end hardware, larger routes are formed
Trueness Level [25]	Matlab	Prevention	Trust Algorithms	PDR rises to 92%	Computation overheads, Trust is solely calculated on the base of PDR
Enhanced Temporal Windowing [26]	NS-2	Detection	Probability and statics of communication parameters	Detection rate is 92-99% for Blackhole attack	Trade-off between threshold and detection accuracy hinders effectiveness

4.1. Collaborative Bayesian Watchdog

Collaborative Bayesian watchdog is a collaborative mechanism for detection of Blackhole attack using equations of finding two parameters of Bayesian filter. In this mechanism firstly, each node calculates the value of two Bayesian variables using equations of Bayesian filters and generate firsthand information about the nature of a particular node. This information is calculated from the information given by the standard watchdog mechanism. Then all the nodes collaborate by sending to each other their respective Bayesian variables. After receiving the required information, the nodes recalculate the values of the two Bayesian variables using a level of trust on the informer. If the node has high level of trust on a particular informer then that node's Bayesian variable will have higher weight. With these each node recalculates the values of Bayesian variables and take decision on whether the node for which the Bayesian watchdog is performed is a Blackhole or not. This is done by continuous Time Markov's chain. When the result comes out to be positive then the node is marked as Blackhole and information about that nodes marking is disseminated in the entire network. The simulation of Bayesian Watchdog is done in NS-2 simulator against standard watchdog and Bayesian watchdog for detection accuracy and speed and Packet delivery ratio. This mechanism reduces the effect of false positive and false negative to greater extent and provides a rapid detection of Blackhole attack. However, this mechanism posed greater overheads due to collaboration of nodes for detection of Blackholes. This large amount of overhead also leads to quick exhaustion of battery of nodes.

4.2. CUSUM

CUulative SUM mechanism provides capabilities of detecting Blackhole attacks in its inception phase without posing significant overheads. In this mechanism, the sequence number associated with nodes in routing table are monitored and if the difference in sequence numbers exceeds some threshold value in a predefined interval then it will raise an alarm for detection of Blackhole. CUSUM is based on some initial statistical distribution that needs some data to start with. So, it provides a training phase to calculate that initial distribution on which detection phase is based. From the training phase, the optimal threshold value that avoids any false positives or true negatives is calculated. Also, in training phase three variants of random sequence Xn, Yn and Zn are produced that defines bound on the rate of change of sequence numbers for nodes. Here, Xn is difference in two successive sampling values of sequence numbers. Zn is mean deviation while Yn is the range of values from 0 to Yn-1 + Zn. After that the threshold value is calculated that is used for Blackhole detection in first iteration of detection phase. In normal phase, at a regular interval of time, the random sequences Xn, Yn and Zn are calculated and from Yn threshold value is calculated which is used for Blackhole detection. If Yn > threshold value, then attack is detected and an alarm is raised to inform other nodes in the network. For any interval in which the attack is not detected, all the random sequences and threshold is recalculated. This mechanism is evaluated in NS-3 simulator against ABM [27], GAODV [28], DCM [29] and SVM [30] on the basis of detection of Blackhole attack, packet delivery ratio and false positive ratio. This mechanism is path breaking in the detection mechanism for Blackhole and Grayhole attack and provides high level of detection without much network overhead. However, a large amount of computational overhead is involved and extra capabilities must be provided in the nodes to efficiently do the computations.

4.3. MBDP-AODV

MBDP-AODV is a mitigation approach for Blackhole. It does the prevention of Blackhole from the communication path establishment by its detection and marking. This mechanism uses mean and standard deviation of destination sequence number in RREP packet for detection of Blackhole. This approach is divided into three phases. First phase deals with calculation of dynamic threshold value for the destination sequence number. The node after sending RREQ packet for a particular destination waits for arrival of few RREP packets. After then, the source node calculates mean of destination sequence number from the received RREP packets. From mean of destination sequence number, the deviation is calculated. This deviation is used as the dynamic threshold value for detection of blackhole attack. For each received RREP packet, the destination sequence number is compared with threshold and if that number is greater than the threshold value, that RREP considered as coming from malicious node. In Second phase detection of Blackhole through SUSPECT and ALERT packets is done. The source sends a SUSPECT packet with same destination sequence number and each intermediate node check for the source of RREP packet for that destination sequence number. If for any intermediate node, it finds the packet to come out from its next hop, it marks that node and broadcast an ALERT packet in the entire network which contains the node ID and suspected destination sequence number. Each node that receives that alert packet marks an entry for that node if not already there in the Blackhole list. Then in third phase, the prevention of Blackhole is done by not allowing that node to participate in path establishment anymore.

This work is tested in NS-2.35 simulator for parameters PDR, throughput and overhead for varying intensities of malicious nodes. This mechanism proves to be good in identifying false negatives and detects the Blackhole in the route establishment phase before any damage done by the malicious node. However, this mechanism imposes greater overhead on the network as compared to other mechanism discussed here due to detection packets SUSPECT and broadcasting of ALERT packet after detection. A smart Grayhole attack that partially drops the packets cannot be detected using this mechanism.

4.4. Trust and Energy Based algorithm

This mechanism modifies the AODV routing protocol by incorporating trust and energy parameters in the route establishment phase. Initially, each node in the network has a trust level 0.5 on each other. After a certain predefined interval, the nodes recalculate trust and energy values. The trust value is calculated in two phases. In first phase, direct trust is calculated on the basis of Packet delivery and Packet Drop Ratio. If for a particular node i, node j has Packet delivery Ratio > Packet Drop Ratio, the direct trust is calculated. If the trust falls below the value 0.5, then node i asks for indirect trust from neighbours and on the basis of indirect trust and direct trust values final trust values are calculated in second phase giving equal weight to both types of trust. After that energy consumption for a particular network in fixed interval is also calculated. In route establishment phase whenever a node needs a path to a particular destination, then it initiates route discovery by sending RREQ packet, to which various nodes responds with RREP packet. The source node waits for a predefined interval for arrival of RREP packets. After the time is expired, the source calculates average trust of path belonging to each RREP packet and selects the path that has highest average trust among the intermediate nodes. The work has been simulated in NS-2 simulator against AODV and AOTDV [31] for parameters PDR, network overhead, latency and energy consumption. The mechanism provides stable paths and least amount of overheads. However, the notion of establishing a path that has greatest average trust may include attacking nodes with low trust but average may comes out to be larger than any other path.

4.5. Distributed Co-Operative Approach

In this mechanism, each node maintains few variables like number of packets sent, number of packets received, packets received for particular destination, packet drop ratio and threshold on packet drop ratio. It controls and detects simple Blackhole attacks easily through increase of packet drop ratio below a certain threshold value. Selective packet drop attack such as Grayhole attack may sometimes confused with intrinsic properties of MANET. So co-operation through opinion of neighbours, neighbours of neighbours and so on is considered before marking the node as selfish Blackhole. Firstly, if a node finds its next hop neighbouring node for a particular destination suspicious, it puts that node in suspect list and sends a REQ packet to neighbours to inquire about the suspected Grayhole attacker. If the neighbour contains that suspected node in its suspect list, it will send a RESP packet. Otherwise, it will further send the REQ to the immediate neighbours to get the desired information. For this probe a random adaptive time is chosen after which the node takes a decision about the suspected Grayhole attacker with the help of received RESP packet, if any. The node calculates the number of RESP packets that are positive and negative regarding suspect attacking node. If 2/3 or more of the total RESP packet inform the existence of that Grayhole suspected attacker in their respective suspect list, then it will mark that node as attacking node and raise a flag to stop communication through that node. This proposed work is tested in NS-2 simulator for the parameters like accuracy in detection of Blackhole and Grayhole attack and throughput. Through this method, with high precision a Grayhole or Blackhole attack can be detected as early as possible. However, the major shortcoming is the broadcasting of SUSPECT packet cause overhead and also after detection of attack; other nodes are not notified about the presence of attacking malicious node.

4.6. Opinion Based Trust Based Scheme

This mechanism uses a notion of trust to determine the trustworthy and formulation of trusted paths through opinion evaluation of opinions sent by other nodes in the network. In this mechanism firstly two parameters RREQ overhead and energy consumption is evaluated by each node for itself. From these two parameters negative trust value is calculated by giving more weight to overheads. After then positive trust value is calculated using from negative trust. Finally, for each node final trust value is calculated and on the basis of final trust value a threshold value is determined through calculation of mean value. After the threshold value is determined, the node asks for opinion from the neighbourhood about a particular node. If the aggregated opinion of the other nodes about a particular node is higher than the calculated threshold then the node under evaluation is marked as trustworthy by a value 1, otherwise value 0 is assigned. However, 0 does not indicate a malicious node. The path is thus formulated only through trustworthy nodes and thus chances of attacks are minimized by avoiding the Blackhole attack. This mechanism is validated using NS-2.35 simulator by comparing this work with a base work of source based trusted AODV [32] against the parameters end-to-end delay, throughput, overhead, energy consumption and packet delivery ratio. This mechanism provides a solid basis to avoid any type of Blackhole or its variant as all the paths formulated only through trusted nodes. However, initially, the network is prone to attacks. Also, high level of overhead is caused through exchange of opinions from the other nodes.

4.7. CORIDS

This is a cluster-oriented reward based Intrusion detection System, in which the entire network is divided into cluster and for each cluster there is a cluster head (CH) that performs the forwarding of packet. The nodes send or receive packets only from their respective cluster heads. Cluster heads has high level of resources and these interact with each other for route formation in a re-active manner. If any node belonging to a particular cluster needs to communicate to another node belonging to some other cluster, then the node sends RREQ packet to CH of its own cluster and then CH forwards that packet to other neighbouring CHs. If the destination belongs to the cluster of some cluster head, it will reply with RREP packet and hence route is established. Each CH maintains six parameters; trust, threshold on trust, PDR (Packet Delivery Ratio), PAR (Packet Arrival Ratio) for nodes in its cluster and PS (Packet Sent) and PR (Packet Received) from a particular Cluster Head of another cluster. The cluster heads forms the path that is of highest trust according to the maintained trust value. The Blackhole attack is detected through PDR/PAR and PS/PR values. In this type of cluster based network, it is assumed no CH is Blackhole and only nodes can act as Blackhole and a node can attack the route establishment only by faking itself as destination. When Blackhole receives as fake destination a packet from its respective CH, then PS value is incremented but PDR is not incremented as the packet is not delivered to the particular destination ID. The CH finds this anomaly and marks that node as Blackhole. The mechanism is validated in Qualnet against MDA [33] for parameters like accuracy in detection and detection speed. This mechanism works well in coping up with false positive and true negatives for any varying mobility speed and scale of the network. However, it has shortcomings is its intrinsic nature in which communication can only take place through CHs thus causing slightly more communication overheads.

4.8. Trueness Level

Trueness level algorithm is a trust based mechanism in which each node maintains a trust value that ranges from 0 to 7. To start with, each node has trueness level 3 for every other node in the network. After a periodic interval of time, each node recalculates the Trueness level for every other node in the network on the basis of the forwarding behaviour of that node. For checking the packet delivery ratio each node acts as a promiscuous node. When through promiscuous mode, the packet drop falls under pre-defined threshold or when the Trueness level of a node falls to 0, then that node is marked as Blackhole by that node and disseminates that information to other nodes. The other nodes on receiving the information about marking of a node as Blackhole compares the trust among those two nodes and then decide whether to mark that node as Blackhole or ignore the information. In path establishment phase, only those paths are selected that has high value of Trueness Level. The Trueness Level of path is equal to the minimum value of Trueness Level among nodes that are involved in that path. Thus, the trust of path is equal to the most unreliable link of that path. This mechanism is simulated in MATLAB 2013a and is compared against W-AODV [34] for parameters like PDR, control overhead, accuracy and reliability of path. This mechanism proves to be efficient in formulating reliable paths and avoiding Blackhole attack. Apart from that it can also help in detection of malicious attacks. However, a large amount of computational overhead is involved and other parameters for calculating trust such as energy consumption and link stability is ignored.

4.9. Enhanced Temporal Windowing

This mechanism provides collection of probability by which a node drops a packet and decides on the basis of this probability that whether the node is malicious or not. This probability is calculated in a time window manner, *i.e.*, after calculating the probability values and using them, in next interval the previous values are discarded. Firstly, probability of CTS [17] and RTS [17] is calculated from probability of drop ratio, collision and mobility of a particular node. These values of probability are calculated by each and every node for every other node in the network. After that for the given interval, the probability of drop ratio is calculated and compared against the pre-defined threshold values. If the probability of drop is greater than or equal to threshold value then the node is considered malicious otherwise a legitimate node. The fixation of threshold value is carefully selected to avoid false positive and true negatives to greater extent. This work is tested in NS-2 simulator for detection ratio and accuracy for different values of mobility speed and node density. This mechanism provides a cross layer detection of malicious Blackhole attack under different circumstances. The temporal window mechanism causes greater overhead due to collaboration among nodes for calculation of threshold value. Also, the value of threshold comes with a trade-off between false positive and detection accuracy.

5. Conclusion and Future Work

Dynamic nature of MANET and inherent design drawback of AODV routing protocol pave the way for Blackhole attack. Many researcher works on mitigation of Blackhole attack with variety o mechanisms. In this paper, we reviewed some of the best methods for detection and prevention of Blackhole attack in AODV routing protocol and critically summarize them for their advantages and shortcomings. In our reviewing process, we observed that the prevention mechanisms isolate the Blackhole and hinder its participation in path establishment. The attackers although somehow break the trust notion and involve themselves in the active path, but these mechanisms have the potential to detect attacking nodes before any substantial damage. However, it may lead to formation of paths that has higher hop count and use of trust notion increases the computation overheads. The detection mechanisms, on the other hand, provide pro-active or re-active detection of Blackhole attack by co-operation or anomaly detection. However, these methods put extra load on network by exchanging huge amount of control packets. We also observed that there is a trade-off between accuracy and efficiency of mechanism and overheads in network and the future researcher must aim at gaining high level of accuracy and network efficiency and minimizing the control overheads on the network.

The area of the research in mitigation of Blackhole attack is still active and wide enough and the researcher must aim at devising efficient mechanism that balances the trade-off. This paper will help the researchers in identifying some of best recent works and realize the importance of these mechanisms in the current scenario. We propose here in this paper after comprehensive reviewing of literature since 2012 that the research should be guided in the direction of avoidance of Blackhole in route establishment as prime objective strengthen by a lightweight detection that is triggered when performance degrades to certain threshold level.

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

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

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

[7] 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.

[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. Rutvij H. 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.

[12] 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)**.

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

[14] 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.

[15] 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.

[16] J. Rutvij H., 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)**.

[17] B.A. Forouzan, “Data Communications and Networking 4th Edition”, Tata McGraw Hill Companies, **(2006)**.

[18] M. D. Serrat-Olmos, “A collaborative bayesian watchdog for detecting black holes in MANETs”, Intelligent Distributed Computing VI. Springer, **(2013)**, pp. 221-230.

[19] C. Panos and C. Ntantogian, “Analyzing, Quantifying and Detecting the Blackhole attack in Infrastructure-less Networks”, Computer Networks, vol. 113, **(2017)**, pp. 94-110.

[20] S. Gurung and S. Chauhan, “A dynamic threshold based approach for mitigating black-hole attack in MANET”, Wireless Networks, **(2016)**, pp. 1-15.

[21] U. Venkanna, J. Krishna Agarwal and R. Leela Velusamy, “A cooperative routing for MANET based on distributed trust and energy management”, Wireless Personal Communications, vol. 81, issue 3, **(2015)**, pp. 961-979.

[22] B. Sharma, “a distributive cooperative approach to detect grayhole attack in manet”, Proceedings of the Third International Symposium on Women in Computing and Informatics, ACM, **(2015)**.

[23] R. Hinge and J. Dubey, “Opinion based trusted AODV routing protocol for MANET”, Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, ACM, **(2016)**.

[24] N. Deb, M. Chakraborty and N. Chaki, “CORIDS: a cluster-oriented reward-based intrusion detection system for wireless mesh networks”, Security and Communication Networks, vol. 7, issue 3, **(2014)**, pp. 532-543.

[25] N. Khanna, “Avoidance and Mitigation of All Packet Drop Attacks in MANET using Enhanced AODV with Cryptography”, International Journal of Computer Network and Information Security vol. 8, issue 4, **(2016)**, pp. 37-43.

[26] L. Sánchez-Casado, “A model of data forwarding in MANETs for lightweight detection of malicious packet dropping”, Computer Networks, vol. 8, issue 7, **(2015)**, pp. 44-58.

[27] M.-Y. Su, “Prevention of selective blackhole attacks on mobile ad hoc networks through intrusion detection systems”, Computer Communications, vol. 34, **(2011)**, pp. 107-117.

[28] S. K. Dhurandher, I. Woungang, R. Mathur and P. Khurana, “GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs”, 27th International Conference on Advanced Information Networking and Application Workshops, **(2013)**, pp. 357-362.

[29] C.W. Yu, T.K. Wu, R. H., Chen and S. C. Chang, “A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks”, PAKDD 2007 Workshops, **(2007)**, pp. 538–549.

[30] J.F.C. Joseph, B. –S. Lee, A. Das and B.-C. Seet, “Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA”, Dependable and Secure Computing, IEEE Transactions on, vol.8, no.2, **(2011)**, pp.233-245.

[31] X. Li, Z. Jia, P. Zhang, R. Zhang and H. Wang, “Trust-based on-demand multipath routing in mobile ad hoc networks”, IET Information Security, vol. 4, issue 4, **(2010)**, pp. 212–232.

[32] A. Pravin Renold and R. Parthasarathy, “Source based Trusted AODV Routing Protocol for Mobile Ad hoc Networks”, ICACCI’12, August 3-5, 2012, Chennai, Tamil Nadu, India.

[33] M.D.A. Hamid, M.D.S. Islam and C.S. Hong, “Misbehavior detection in wireless mesh networks”, International conference on Advanced Communication Technology, **(2008)**, pp. 1167–1169.

[34] T. Varshney, T. Sharma and P. Sharma, “Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network”, IEEE International Conference on Communication Systems and Network Technologies, **(2014)**, pp. 217-221.