Democratic Detection of Malicious Behaviour in MANET: A Voting Process

EO Ochola
School of Computing
University of South Africa
Pretoria, South Africa
ocholeo@unisa.ac.za

MM Eloff
Institute for Corporate Citizenship
University of South Africa
Pretoria, South Africa
eloffmm@unisa.ac.za

JA van der Poll
Graduate School of Business Leadership
University of South Africa
Midrand, South Africa
vdpolja@unisa.ac.za

Abstract— **Wireless MANET presents new security problems in comparison to the conventional wired and wireless networks, as it is more vulnerable to malicious attacks due to its unique features. The MANET routing protocols require that the mobile nodes that form such temporal network cooperate with each other to achieve the desired routing purpose for the exchange of information amongst the participating nodes. However, the cooperation cannot be realised where network nodes exhibit malicious operations. The MANET characteristics and applications make it difficult to have a centralised security management entity. Furthermore, the implementation of Power-Aware routing protocols complicates the possibility of relying entirely on watchdog mechanisms to safeguard the network against Black-Hole attack. In addition, the watchdog's eavesdropping operation violates the TCP protocol rules, and requires buffering of large amount of packets during the monitoring process, which results to extra overheads. This paper proposes an algorithm which utilises Cluster-Heads and votes from neighbourhood nodes to detect and eliminate malicious nodes. It addresses challenges posed by Power-Aware routing protocols and watchdog approaches in detecting Black-Hole attack, thereby increasing nodes' availability and the overall network performance.**

Keywords-MANET; black-hole attack; security; power-aware routing; watchdog

I. INTRODUCTION

Security in mobile ad hoc network (MANET) [1][10] is a necessity for proper functioning of the network's routing and packet forwarding, the two of which are the MANET's core basic functions. Secure MANET operations require the integration of security countermeasures into the functions as early as during design stages. Whereas wired and cellular networks have fixed infrastructures that provide security support to the routing, packet forwarding and network management, MANET lack such infrastructure and requires that all network nodes act as both hosts and routers, cooperatively supporting the network functions. However, the cooperation is not guaranteed since not all nodes can be trusted to function correctly according to underlying routing protocol. The network nodes are required to be fair and operate correctly while executing critical network functions, which require their cooperative participation. However, a fare share performance by MANET's nodes poses a challenge due to device power resource constraints. Recent research works have identified black-hole attack as a new type of malicious misbehaviour in MANET, with countermeasures to eliminate non-cooperative nodes.

MANETs lack prior trust of its participating nodes since they are free to join and leave such network at will. This limits the application of existing classical network security techniques based on access control and authentication in dealing with black-hole type attack, hence the application of cooperative security techniques as the best solution option in ensuring MANET security [1]. Cooperative security techniques allow for the detection of black-hole attack misbehaviours through the collaboration of the network nodes with the assumption that majority of the nodes are trustworthy. In this paper, an ad hoc on-demand distance vector (AODV)-based routing protocol is presented to detect black-hole attacks in MANET with the support of cluster-heads and genuine neighbors to a suspected black-hole node.

Section II of this paper presents the black-hole attack, its operations and AODV protocol. In section III, the related work done by the different authors are presented. Section IV presents the proposed algorithm including attack solution framework with possible black-hole attack scenario. Section V and VI present the simulation results and the conclusion respectively.

II. BLACKHOLE ATTACK ON AODV PROTOCOL

A. *AODV routing protocol operation*

Designing MANETs' routing protocols remain an uphill task [1]. Due to rapid topological and mobility changes in MANETs, the applications of wired network protocols are rendered unsuitable. Current existing studies appertaining to MANET routing challenges have been carried out with the assumption that there exist no malicious misbehaviours among the active nodes, i.e., every node is trusted.

Due to better performance of reactive routing protocols, current research efforts in designing MANET secure routing protocols have mainly focused on on-demand protocols, and more specifically to AODV due to its popularity [1][2][3][6], where routes are discovered only when needed and kept only when active. Reactive routing protocols perform better than their proactive counterparts due to low overheads in less dynamic networks and are similarly efficient in performing route maintenance in dynamic networks with frequent topology changes.

On-demand routing protocols flood *Route Request* (RREQ) when discovering new routes. The response from a single RREQ may lead to the discovery of multiple routes to a specific destination node. AODV differs from other on-demand protocols due to its utilization of destination sequence number (DestSeqNum) in determining fresh routes. A node's DestSeqNum value is updated only if it receives a packet with a greater DestSeqNum, a condition violated during black-hole attack.

The freshness of a discovered route is determined by the value of the DestSeqNum. An intermediate node generates a *Route Reply* (RREP) if it has the needed route under discovery; otherwise, the RREQ is forwarded to the next-hop node until it either reaches an intermediate node with a valid route or the destination node, which then respond with a RREP to the source node, after which the source responds by sending the data packets through the established path. Whenever an intermediate node detects a path break, it updates the end nodes by sending a *Route Error* message (RERR) with the hop count set to ∞. Maliciously, black-hole nodes do not give a path-break notification. Hence, no further attempt by the source to resubmit the consumed packets.

B. *Power-Aware Routing in MANETs*

MANETs are characterised by constrained resources which include operational battery power; given the size, portability and weight of hand-held communication devices. Therefore, the application of routing schemes which take into consideration the device power levels are preferred as they efficiently utilise the available energy, hence, a prolonged network lifetime.

Minimum Energy Consumption per Packet is one of the metrics used to address limited battery power challenges in MANET [1][4]. This metric minimises the total power consumed while sending a packet from source node to the destination, which is the sum of power consumed per hop along the route, and is similarly a function of the distance between the nodes that form the link.

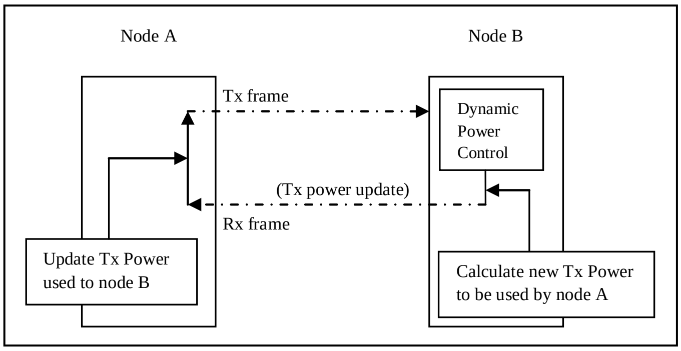
Node A
Node B
Tx frame
Dynamic Power Control
(Tx power update)
Rx frame
Update Tx Power used to node B
Calculate new Tx Power to be used by node A

Figure 1. Dynamic transmission power control feedback loop.

Transmission power greatly influences the reachability of a node and thus the range covered by it. The *dynamic power transmission* schemes can be utilized by black-hole nodes to launch the forwarding disruption attack (range attack) as noted in [14]. Recent works in [4] indicates a possible power saves and a prevention of unnecessary energy wastage by making a proper nodes' power levels selection in wireless MANETs. *Dynamic Power Adjustment* mechanism is one of the solutions proposed to calculate the optimum transmission range [4]. This involves the calculation of the minimum transmission power that a node requires to reach each of its next-hop node (neighbor), based on the signal strength of the previously received control packet during neighbor and/or route discovery process, as in Fig. 1. While the control packets are transmitted at the maximum transmit power, the data packets are transmitted at the calculated minimum transmission power. This makes it impossible to successfully use the watchdog mechanisms to detect black-hole attack's malicious misbehavior in such power-aware routing protocols, if embedded in MANET's AODV routing protocol. While the watchdogs will be able to listen to transmitted control packets, they may not be able to list to the transmitted data packet due to the dynamically adjusted minimum transmission power, resulting to false positive detections of black-hole nodes.

C. *Blackhole Attack and Watchdog Mechanisms*

Malicious Nodes can disrupt routing protocol's correct functionalities through modification and fabrication of routing information, and impersonation of genuine nodes. Recent research studies [7][10][13] have discovered a new type of MANET's AODV routing protocol's attack known as black-hole.

In black-hole attack [2][5][6], a malicious node responds with RREP with an indication of having the most recent and shortest path to the intended destination node. In flooding-based routing protocols, e.g., AODV, the attacker quickly responds to the received RREQs with respective RREPs with indications of having fresh and extremely short routes. If such RREPs are received by source nodes before the reception of normal RREPs from non-malicious nodes, then forged routes get created. Once the malicious node (black-hole) inserts itself between the communicating nodes (source and destination nodes) as a relaying intermediate node, it is then able to intercept, modify and drop the packets passing through it [5][8]. The malicious behavior of black-hole nodes can severely degrade network performance [2] and eventually partition the network by simply not participating according to the routing operation.

To mitigate the decrease in the throughput due to the existence of a black-hole node in MANET, watchdogs that identify misbehaving nodes and a path-rater that helps routing protocols to avoid these nodes are used [8]. When a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by listening promiscuously to the next node's transmissions. If the next node does not forward the received packet, its failure tally is increased by the watchdog. A node is then determined as a misbehaving node by the watchdog if its failure tally goes beyond a pre-determined threshold. The path-rate then avoids such node in the future communication. Each network node runs a path-rater, which links the knowledge of a misbehaving node to its reliability before picking the most reliable route for data forwarding. Each node maintains a rating for every other known network node. The path metric is then calculated by averaging ratings of all the nodes in a given path [5][8].

The watchdog technique has its own advantages and weakness. The watchdog's weaknesses are that it might not detect a misbehaving node in the presence of:

(1) Ambiguous collisions: which prevents it from overhearing the transmission from the next node;

(2) Receiver collisions: where a watchdog can only tell whether a packet has been sent to an intermediate node, but it cannot tell if the intermediate node received it or not;

(3) Dynamic transmission power control: where an intermediate node could limit its transmission power such that the signal is strong enough to be overheard by the next-hop node but too weak to be received by the monitoring watchdog [4][8];

(4) False misbehavior: this occurs when a node falsely reports other nodes as misbehaving;

(5) Partial dropping: a node can circumvent the watchdog by dropping packets at a lower rate than the watchdog's configured minimum misbehaving threshold.

A solution to the above watchdog weaknesses in detecting black-hole node in the presence of a dynamic transmission power control scheme is presented in section IV.

III. Related Work

Various related black-hole attack detection approaches have been proposed and discussed [2][9]. The following discussion reviews those under the categories of *passive feedback based schemes*, *acknowledgement based schemes* and *reputation based schemes*, which are directly related to the proposal in section IV:

(i) The requirement that every intermediate node to include the identity of the next hop node towards the destination in its RREP packet while responding to every RREQ packet is presented [2]. The source node then contacts the next-hop node to verify if indeed a route exists to the destination before sending the data packet. Otherwise, the intermediate node is marked as malicious and eliminated in the future communications. This is found to be having drawbacks such as the process of RREP verification and the overheads resulting from the next hop node validity responses. Furthermore, this presents the possibility of using the same black-hole node as a relay node during the verification process which might compromise the validation process.

(ii) A modification of AODV protocol to include data routing information table (DRI) and a cross checking process is discussed [9]. Each network node maintains its DRI table with information as to whether an intermediate node has transferred data to its neighbors and identifies misbehaviors. However, the cross checking process comes with overheads which increases end-to-end delay, as it involves the participation of every node. Furthermore, the approach may not be applicable in dynamic transmission power control routing protocols, as the transmitted data packets may not be overheard due to transmission power variations, resulting into false positive identifications.

(iii) A watchdog and path-rater scheme for malicious node detection in MANET is presented [5][8][12]. The misbehaviors are captured through eavesdropping on the transmissions of the next-hop node. However, the buffering of every overheard data packet by the watchdog comes with additional memory space and computational process for packet matching. The inappropriateness of such scheme in the presence of limited transmission power is also noted.

(iv) A scheme that verifies the value of every RREP's sequence number is addressed. Should an intermediate node generate a RREP with a higher sequence number than a given threshold value, then such node is flagged as malicious. However, a black-hole node may decided to send all its RREPs with a sequence number equal to the set threshold value and avoid any detection, leading to false negative identifications [8][9].

(v) An approach that requires that many RREPs be received before sending a data packet through one of the routes with repeated next hop nodes is presented [2]. However, in the absence of paths with repeated next hop nodes, the scheme chooses one of the available paths randomly, which may be a path with a black-hole node.

(vi) A trust manager aided watchdog approach, in which all network nodes act as watchdogs with the trust manager making detection decisions based on a given threshold defaulting, is discussed [8][11]. The participation of every node as a watchdogs increases network traffic, yet the approach still falls short of correct detections in transmission power variation scenarios.

(vii) A two-to-three hop acknowledgement based schemes are discussed [8]. Each node asks its two hop neighbor to send back a receipt acknowledgement. This may occur continuously for every packet forwarded or randomly. The continuous acknowledgement and the involvement of every node along the path result to excessive overhead, while the random approach may fail to detect selective packet dropping. And even if misbehavior is detected, there still exists a need to verify which one between the one hop node and the two hop node is malicious.

(viii) Reputation based schemes require that a historic observation about the behavior of a node be kept to determine whether it is trustworthy or not [8][11]. Each node must form an opinion regarding the other nodes based on their observed past behaviors. These schemes require excessive traffic exchange for sharing the reputation information between every node, and are not efficient in large MANETs. The monitoring process may use the watchdog's overhearing technique, which fails in the presence of dynamic transmission power routing protocols.

The above discussed solutions intended to avoid black-hole attacks in MANET have varying defects leading to possible false negative and positive detections, with all the watchdog approaches failing to function correctly in the presence of embedded dynamic transmission power schemes in the existing MANET routing protocols (e.g., AODV). Most of the existing solutions rely on the watchdog technique to ensure the correct forwarding of packets by the neighboring nodes. However, this technique suffers from certain weakness mentioned in section II and analyzed in section III, particularly when power control is applied.

IV. Proposed Solution Approach

Based on the watchdog technique's weaknesses discussed in section II above, the proposed cluster-head aided neighbor voting technique is intended to detect black-hole attack in the presence of dynamic transmission power control that is executed by the existing power-aware routing protocols in MANET.

Algorithm: CLUSTER-HEAD AIDED VOTING BLACK HOLE DETECTION

```
//Cluster-heads form a closed communication, i.e., any Cluster-head is reachable to any other, either in one hop or via relay through intermediate Cluster-heads
//A Cluster-head has neighborhood list of the nodes within its coverage and reachable to the cluster-set nodes in one hop
//Cluster-heads and destination nodes are normal nodes (non malicious nodes)
// vote=0: 0, all nodes are considered non malicious initially
begin
1.  on source node S receiving the first reply (RREP) for the route discovery process that it has launched,
2.  if the RREP generator node M is either the destination node or a cluster-head then
        Send data normally under classical AODV routing, without initiating any detection process // M is normal node
    else
        Send the data and immediately send out a special message to inform your Cluster-head of the ongoing transmission to launch detection process // M may be malicious (Black-hole)
    end if
3.  on an intermediate node X receiving a forwarded packet,
4.  if the packet is a special message then
        if X is the M's Cluster-head then
            if X received data packet from M within the time interval $T_{0+k}$ then
                M is normal node // detection process is terminated
            else
                Send vote request message to M's neighbors // the vote request contains the RREP generator ID, and the time period $t_{0+k}$
                if vote=1 is received then
                    M is normal node // M forwarded the data which was received by the next-hop neighbor along the route, which it acknowledged by sending vote=1to the Cluster-head, and no further detection process is carried on
                else // all votes received are vote=0, and a vote=0 is registered by the Cluster-head for M as one additional possible misbehavior
                    Vote=0++ // increment the malicious possibility of a node
                    if accumulated vote=0 for M is greater than threshold then
                        Mark M as malicious node (Black-hole)
                        Send Alarm packet to exclude M from participating in the network
                    else
                        M is normal node // the drop of the packet may have been normal as a result of either packet collision or traffic congestion, and detection process is terminated
                    end if
                end if
            end if
        else // X is not M's Cluster-head
        Forward packet // X is an intermediate node and forwards special message towards the M's Cluster-head, until the Cluster-head is reached
        end if
5.  else // the packet is data
        if X is destination then
        Consume data // no detection process is carried out
        else //X is an intermediate relay node
        Forward packet // towards destination along the route
        end if
6.  end if
end
```

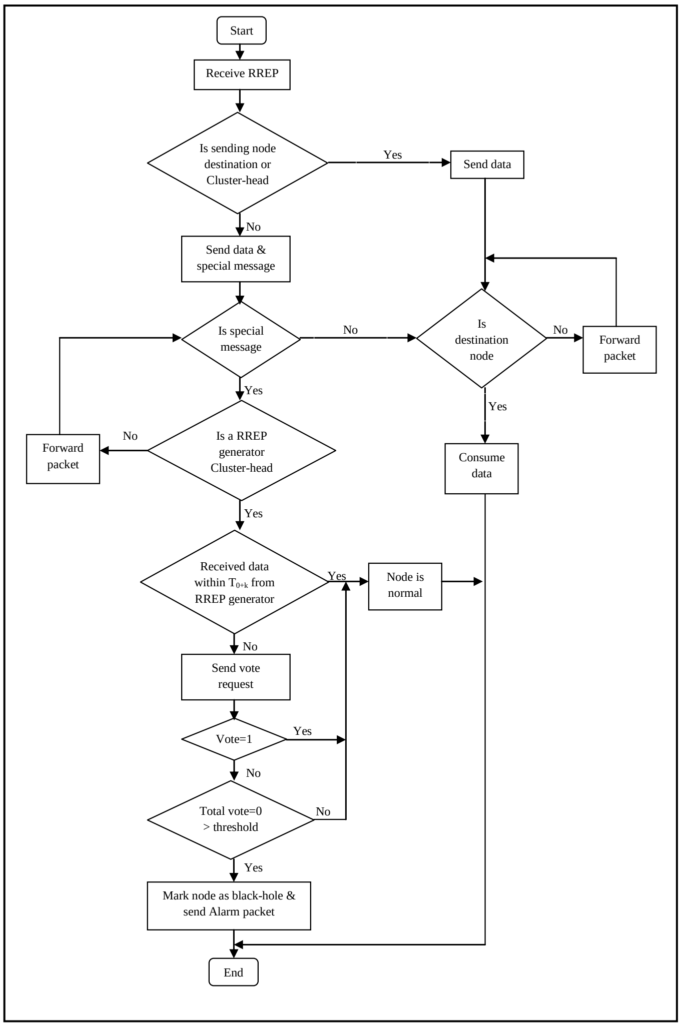

Figure 2. The proposed algorithm framework.

The algorithm is cluster type independent and can operate with any category of clustering algorithms in MANET, which include [15]: identifier-based clustering, connectivity-based clustering, mobility-aware clustering, low cost of maintenance clustering, power-aware clustering, and combined-weight based clustering, provided the applicable assumptions are taken into consideration during Cluster-head selection process. Figure 2 present the proposed algorithm's framework. If a suspected black-hole node M happens to be under the coverage of more than one Cluster-head, as the case of nodes D, S, 7, 8, 10, 12, 13, 14 and 17 in Fig. 3, then all the affected Cluster-heads consult each other to share their votes concerning node M during the time interval T_{0+k}. This takes into consideration a situation where the genuine next-hop neighbor is out of the range of the suspected black-hole's known Cluster-head. The affected cluster-heads will then update their votes register after receiving other Cluster-heads' votes besides the votes from the M's neighbors within their coverage, before marking node M as black-hole based on an acceptable defaulting threshold. This reduces possibilities of false positive detections, and ensures that any data forwarded by node M and received by any of its next-hop neighbor registers a *vote=1* vote.

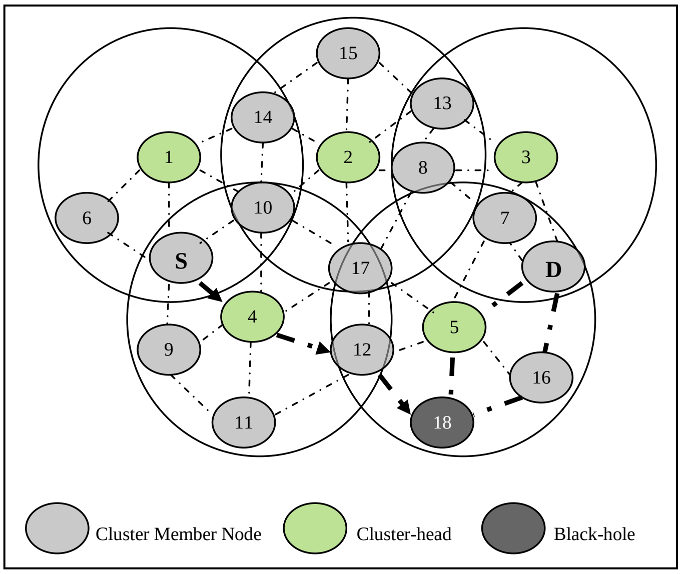

Figure 3. Black-hole detection voting process.

Figure 3 illustrates the proposed Cluster-aided black-hole detection voting process. Source node S intends to send data to destination node D and broadcasts RREQ according to classical AODV routing protocol. The Black-hole node 18 sends RREP to node S as a response to the RREQ with the highest sequence number (fresh route) and a hop-count of 1(shortest path). Node S then sends data packet to node D via node 18 (Black-hole). But since node 18 is neither the destination nor a Cluster-head, S sends *special message* to node 5 (node 18's Cluster-head) to perform the Black-hole detection within a given time interval T_{0+k}, in which node 18 should have received the data packet and forwarded it. Node 18 has got two possible shortest paths to D according to AODV protocol, i.e., either path 18-5-D or 18-16-D. On receiving the *special message* packet by node 5, it checks if it has received any data packet from node 18 within time T_{0+k}, in which node 18 will be considered a normal node if it forwarded the packet. Otherwise, node 5 will launch the detection process by sending *vote request* message to node 18's neighbors (node 12 and 16). Either node 12 or 16 (in this case 16) will respond with *vote=1*, regardless of a Power-Aware protocol in use, if node 18 behaved normally by forwarding the packet towards D, and in the absence of collision. In that case, node 5 will consider node 18 a normal node. Otherwise, both node 12 and 16 will respond with *vote=0* vote, implying that node 18 may be a Black-hole. Node 5 then check the number of times vote requests for node 18 has been made in which the responses received was a *vote=0* vote. It then mark node 18 as Black-hole if the *vote=0* responses exceeds a set threshold. Otherwise it increases the number of *vote=0* received for node 18 by 1 (possible Black-hole) and consider node 18 normal, awaiting next detection process, as the lack of the received data packet could have been due to normal channel errors.

Based on the voting detection process in Fig. 3, a Black-hole node will be accurately detected within the first attempt to drop data packet. The participation of the affected Cluster-heads within whose range the Black-hole falls will assist in eliminating cases of false positive detections, where the next-hop along the forwarding route is out of the detecting Cluster-head's range. And since the MANETs' Transmission Power-Aware protocols operate such that the data packet's transmission power should enable it to be received correctly by the intended next-hop node, the packet will be received and a suspected node will not be falsely marked as Black-hole, a scenario which may not be correctly addressed by watchdog schemes, where the transmission power is high enough to make the packet be received my next-hop node but too low to be overheard by the watchdog.

V. Simulation Results

OMNeT++ [16] simulator is used to simulate the proposed solution. Throughput is the metric used to compare the appropriateness of the proposed approach. The validation is done by comparing the network performance in varying conditions, that is; under the classical AODV routing protocol without black-hole attack, a black-hole attacked AODV without a detection and elimination mechanism, and finally a black-hole attacked AODV with the proposed detection algorithm. Figure 4 shows that the proposed algorithm improves the throughput of the network under black-hole attack.

Figure 4 confirms the reactive approach of the proposed security solution scheme, as it can be seen that the performance of the proposal (black-hole voting detection AODV) does not match that of an attack free (AODV), since the black-hole nodes are only detected and removed after they have performed at least one malicious behavior incidence. However, its performance is far much better than that of a network without any attack detection and elimination (black-hole AODV).

VI. Conclusions

Power-aware routing protocols may result to a higher level of black-hole attack in MANET, where a misbehaving node could limit its transmission power such that the signal is strong enough to be overheard by the monitoring (watchdog) node but too weak to be received by the true recipient, thereby not forwarding the data packet to the next-hop node along the route to the intended destination, impacting as if the packet was dropped altogether. Similarly, the transmission power may be reduced such that it is high enough to correctly transmit data packet to the intended next-hop node, but too weak to be overheard by the watchdog, resulting to false positive detections.

The proposed approach detects a black-hole node which either drops all the received data packets or performs a selective dropping of packets destined for specific destinations. It does not make use of the eavesdropping techniques used by watchdog mechanisms and therefore is applicable even in situations where power-aware routing protocols are in operation. The fact that not every node participate in every detection process initiated by a source node, leads to reduced delays and overheads, hence, an improved throughput.

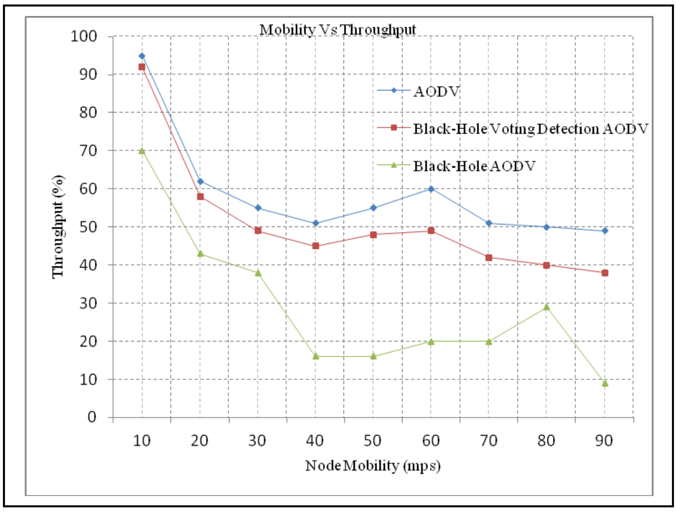

Figure 4. Effect of black-hole attack on the network throughput.

A future work is envisaged towards coming up with an efficient proactive solution i.e., that which identifies a black-hole in advance before doing any damage to the network.

References

[1] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, Mobile Ad Hoc Networking, IEEE Press, New Jersey: Wiley - Interscience, 2004.

[2] E. O. Ochola, M. M. Eloff, and J. A. van der Poll, "Mobile Ad-hoc Network Security Challenges under AODV Routing Protocol", International Network Conference (INC 2012), pp. 113-122, July 2012.

[3] C. Siva Ram Murthy and B. S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall, 2004.

[4] E. O. Ochola, D. Chatelain, and A. Kurien, "Dynamic Power Control On-demand Routing Protocol", In Proceedings of the Southern African Telecommunication Networks and Application Conference (SATNAC 2007), September 2007.

[5] A. Mishra, Security and Quality of Service in Ad Hoc Wireless Networks, Cambridge University Press, 2008.

[6] Y. P. Singh, P. K. Singh, and J. Prakash, "A Survey on Detection and Prevention of Black Hole Attack in AODV – based MANETs," Journal of Information, Knowledge and Research in Computer Engineering, vol. 2, no. 2, pp. 359-365, 2013.

[7] C. Garg, and P. Rewagad, "Analysis of Black Hole and Worm Hole Attack on AODV Routing Protocol in MANET," Asian Journal of Computer Science and Information Technology, vol. 3, no. 2, pp. 9-12, 2013.

[8] S. Djahel, F. Nait-abdesselam, and Z. Zhang, "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges," IEEE Communications Surveys and Tutorials, vol. 13, no. 4, pp. 658-672, 2011.

[9] I. Woungang, S. K. Dhurandher, R. D. Peddi, and I. Traore, "Mitigating Collaborative Blackhole Attacks on DSR-Based Mobile Ad Hoc Networks," In: J. Garcia-Alfaro et al. (Eds.): FPS 2012, LNCS, vol. 7743, pp. 308-323, 2013.

[10] J. A. Patil, and N. Sidnal, "Survey – Secure Routing Protocols of MANET," International Journal of Applied Information Systems (IJAIS), vol. 5, pp. 8–15, March 2013.

[11] B. Yang, R. Yamamoto, and Y. Tanaka, "Historical Evidence Based Trust Management Strategy against Black Hole Attacks in MANET," ICACT2012, pp. 394-399, February 2012.

[12] S. Djahel, F. Nait-Abdesselam, and A. Khokhar, "An Acknowledgment-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol," ICC '08 Proceedings, pp. 2780-2785, May 2008.

[13] S. Agrawal, S. Jain, and S. Sharma, “A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks,” Journal of Computing, vol. 3, no. 1, January 2011.

[14] P. Joshi, G. S. Chandel, and S. Joshi, “A Survey on: Resource Consumption Index of Denial of Service Attack in MANET,” International Journal of Science Engineering and Technology Research (IJSETR), vol. 2, no. 2, pp. 314-318, February 2013.

[15] R. Agarwal, and M. Motwani, “Survey of Clustering Algorithms for MANET,” International Journal on Computer Science and Engineering, vol. 1, no. 2, pp. 98–104, December 2009.

[16] A. Varga, and R. Hornig, “An Overview of OMNeT++ Simulation Environment,” In Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops (Simutools ’08), Marseille, France, pp. 1-10, March 2008.