Volume 8, No. 4, May 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

HSCT: A Hybrid and Secure Clustering Technique for Detection of Black hole Attack in Mobile Adhoc Networks

Harmeet Singh
Assistant Professor, Dept of CSE
SBBS University, Punjab, India

Opinder Singh*[1]& Dr. Jatinder Singh[2]
[1]Research Scholar, IKG Punjab Technical University
Kapurthala, Punjab, India.
opindermca2008@gmail.com

***Abstract*--Mobile Adhoc Network (MANET) is a dynamic network with large number of mobile nodes .As the traffic increases over the MANET, it will leads to number of problems like congestion and packet loss. This congestion and packet loss problems occurs due to the attacks in MANET .Out of the various attacks black hole attack is most dangerous attack which drops all of the packets received from the source node and which act as a black hole in the universe. In this paper we are providing solution against this attack. We propose a new hybrid and secure clustering technique for detecting and isolating black hole attack in MANET. This technique firstly detect the black hole attack by using threshold values against different parameters, after this clustering approach is used for secure path from source to destination by reducing overhead in the network. Most of existing mechanisms are not as efficient because by isolating black hole attack overhead is increased. A HSCT approach has remarkable advantage over these existing techniques. We simulate the proposed technique by using ns2 simulator and proved that our technique effectively detect the black hole attack in terms of throughput, packet loss, overhead, delay. In the last section of paper we deliberate possible future work.**

Keywords--Black hole attack; Mobile adhoc networks; HSCT;clustering; NS2.

I. INTRODUCTION

Mobile Ad hoc Networks (MANET) are the wireless networks of mobile computing devices without any support of a fixed infrastructure. The mobile nodes in a MANET self organize together in some arbitrary fashion. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time [1]. These networks can be applied between persons or between vehicles in areas which are depleted of fixed infrastructure. Two nodes can directly communicate with each other if they are within the radio range. If the nodes are not within the radio range they can communicate with each other using multi hop routing. The wireless link between the nodes in mobile networks is highly vulnerable. This is because nodes can continuously move causing the frequent breakage of the link. The power available for transmission is also strictly limited [2]. The topology of the network is highly dynamic due to the continuous breakage and establishment of wireless link Nodes continuously move into and out of the radio range. This gives rise to the change in routing information. The network is decentralized; where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves i.e. routing functionality will be incorporated into mobile

Fig. 1: Mobile Ad hoc network.

nodes. MANET is more vulnerable than wired network due to mobile nodes, threats from malicious nodes inside the network. Because of vulnerabilities, MANET is more prone to malicious attacks. MANET has following vulnerabilities [3, 4]:

- Lack of centralized node
- Scalability
- Limited power supply
- Adversary inside the Network
- Limited Resources
- Dynamic topology
- Bandwidth constraint
- No predefined Boundary

MANET often suffer from security attacks because of its features like open medium, dynamic topology, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats. Various attacks on different layers of MANET are shown in the following figure 2.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

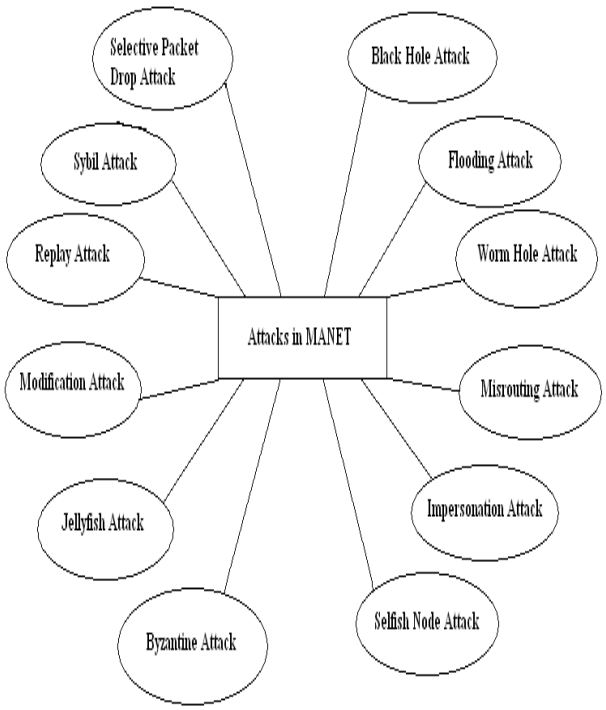


Fig. 2: Different types of attacks in Mobile Ad hoc network.

Black hole attack is one of the main attack in network layer of MANET. In this type attack, malicious node acts as a black hole in the universe. A malicious node drops all of the data packets received from source node without transferring to the target node. In this attacker node represents itself as a node with smallest path to target node by minimum hop count and maximum sequence number [5]. After getting route from source to destination, node start dropping all of the packets received from the source node. In the following figure 3 node 3 is malicious node creating black hole attack in MANET.

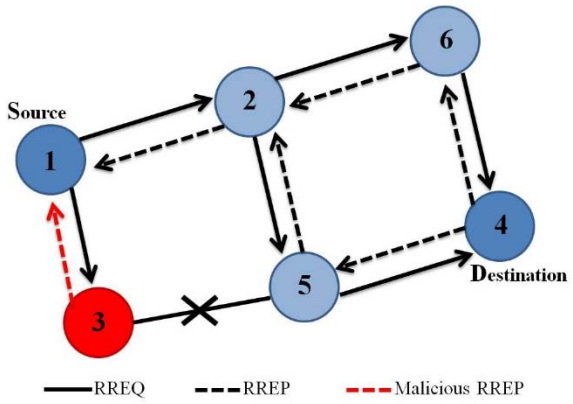


Fig. 3: Black hole attack in MANET

A variety of approaches are available to tackle with black hole attack. In this section of paper, we will discuss a Hybrid and Secure Clustering Technique for Detection of Black hole Attack in Mobile Adhoc Networks and also prove that our technique enhanced the performance of network in the terms of overhead, throughput, packet loss and delay.

II. RELATED WORKS AND PROBLEM FORMULATION

In this section of the paper, we have presented related works in the literature for tackling with black hole attack in MANET. A detail study of these proposed techniques help us in formulation of problem and its possible solution.

Anand A. et al. [6] in their paper propose a hash function based intrusion detection system for detecting and preventing from black hole and gray hole attacks. MANET is protected from black hole attack by rejecting first optimal path and integrity of the data is maintained by using hash function. D. et al. [7] proposed a modified layered cluster based approach for prevention from black hole attack in MANET. This approach works on the basis of trustworthiness principle of the network. All of the nodes in the network are divided into number of clusters. Cluster head of one cluster interact with cluster head of the other cluster for establishing the secure path from source to destination. Each cluster head in the network has its own responsibility to takes care of all its member in its cluster. N. Jaisankar et al. [8] provide a novel approach for isolating black hole attack in MANET by providing minimum additional delay and maximum packet delivery ratio. The proposed approach is based on promiscuous mode to detect and isolate malicious node. Subhashis Banerjee et al. [9] propose an AODV based black hole attack Mitigation technique in MANET without modifying the packet format of AODV and without introducing any black hole detection packets. Ankita V. Rachi et al. [10] propose a novel approach EBAODV which works on the basis of leader nodes for detection of black hole attack This approach is responsible for increasing throughput and packet delivery ratio.

Dasgupta et al. [11] provide a coloured petri net model for detection and prevention from black hole attack in MANET. This model modifies number of properties and provide better results as simulated through a CPN tool. Satoshi Kurosawa et al. [12] in their work provide a dynamic learning based technique for detecting black hole attack in MANET. This technique is based on using dynamically updated training data for isolating malicious node. Jain et al. [13] makes use of AODV's sequence number for mitigation of black hole attack in MANET without modifying the packet format of AODV. All the detection and prevention are performed by originator node without relying on other nodes in the network. Bo Sun Yong et al. [14] makes use of neighbor set based along with the routing recovery protocol for mitigating black hole attack in MANET. Simulation results show that this technique reduced the overhead of the network. X. Li et al. [15] in their work present a trust based on demand multipath routing for isolating black hole attack. A node's trust is based upon its packet forwarding ratio. In this method a source node establishes multiple trustworthy paths to a destination in single route discovery.

PracheeN.Patil et al. [16] presents a new approach based on route caching for detecting and preventing from black hole attack in MANET. In this approach, firstly black

hole node is detected and then its node id is passed to the function of DSR. Vimal Kumar et al. [17] introduce an enhanced AODV routing protocol for detection of black hole attack in MANET. This adaptive approach is based on a coming route reply table (CRRT) which stores the value of RREP packet. CRRT stores the information about originator IP address, destination IP address, next hop, destination sequence number, hop count and life time. Amole A. Bhosle et al. [18] makes use of watchdog mechanism for detecting multiple black hole attacks in MANET. This mechanism improves throughput and packet delivery ratio of the network. Muhammad Imran et al. [20] provides detection and prevention technique for isolating black hole attack in MANET. In this technique DPS nodes are deployed in the network which continuously monitor the performance of their neighbor nodes. These DPS notice the RREQs broadcasted by its neighbor nodes. After checking number of parameters of its neighbor nodes, DPS node declares that suspicious node as black hole node and then broadcast threat message in the network.

Ranajoy Chatterjee et al. [21] in their work present a technique for isolating black hole attack in MANET by using node stability system. This proposed mechanism can successfully identify and isolate singular and co- operative black hole nodes from the network. Khalil I. Ghathwan et al. [22] introduce an artificial intelligence based technique for preventing from black hole and cooperative black hole attacks in MANET. This is an integrated approach based on both A* and Floyd-Warshall's algorithms This mechanism works on the basis of finding shortest secure path for AODV (SSP-AODV). M. Rajesh Babu et al. [23] in their paper provide a novel honeypot based detection and isolation approach for preventing from black hole attack in MANET. This proposed approach reduces the overhead, packet drop ratio and routing load of the network. Kamatchi et al. [24] introduce a new mechanism based on secret sharing and random multipath routing for preventing from black hole attack in MANET. This packet reduces the packet delay and packet drop ratio in the network.

As we have discussed various techniques for detecting black hole attacker nodes in MANETs, but there are various limitations regarding decreased performance in some parameters while improving in another parameters. In this paper we propose a new HSCT for detecting black hole attack in MANET. While designing the intrusion detection system for fully addressing black hole attack in MANETs, the first step is to study the various characteristics of black hole attack. There is also need to study route replying nodes under various parameters for detecting attacker nodes. We focus our research on a view of increasing performance against packet loss, throughput and overhead by detecting and isolating black hole attack in MANET. This paper presents a new hybrid and secure clustering technique based on route request reply time, hop count and sequence number for detecting black hole attack in MANET. This detection technique is extension to the AODV protocol by combining benefits of clustering technique to increase the performance under various parameters.

III. PROPOSED WORK

In our proposed work, we detect the black hole attack from MANET with increased overhead. In this technique, first of all route Reply Times (RT) from various nodes is calculated based on the reply to the route request parameter. This time is compared with the waiting time (WT). This waiting time is the average time of various nodes in the network which are replying with route to destination node. After getting route reply messages from all of the intermediate nodes, if RT of the particular node is less than WT, then the next step is to verify whether this intermediate node is malicious node or not. This node needs to be checked under various parameters for verifying it is malicious node or not. In this technique, a malicious table is obtained which is based on the previous traffic record of the network. If any node found to be a malicious node, then its information is stored in the malicious_table. The node is declared malicious based on the various parameters. In the proposed technique, if any node fails under different parameters and also represents the properties of black hole attack then it is declared as a malicious node and its ID is included in the malicious_table, so that in future this node is isolated from the network. If RT<=WT then node_id is compared with all IDs in the malicious table, if it matches then node is declared as malicious node and route_reply from the malicious node will be discarded. If route replying node is not in the malicious_table then next step is to calculate distance_time value. This value should be minimum and match with the expected hop count value. If it does then store that value in the dt_table, otherwise discard that route_reply. If next hop confirms that replying node has a path, then node_id and its seq_no. is stored in the RREP table, otherwise node_id and its seq_no. are stored in the malicious table. Once all of the sequence numbers are verified, then select node with the highest seq_no. from the RREP_table. This node is treated as cluster head in the network. The algorithm and flow chart of the proposed technique are

A. ALGORITHM

Step 1: Get current time (Time at which route request message is sent)
Step 2: Get waiting time (WT).
Step 3: While (RT<=WT).
Verification of route reply messages are done by various step verifications.
Step A: Check for malicious node.
i. After getting route replies from intermediate nodes, check the malicious_table for malicious node_id which is formed on the basis of previous traffic.
ii. If node_id is matched with the malicious_table, then discard the route reply.
iii. If node_id is not found in the malicious_table, then go to step ii.
Step B: Check the distance_time value.
i. If distance_time value matches with expected hop count value, then store that value in dt_table and go to step C.
ii. Else discard the route reply.
Step C: In this sender node ask the next hop that node replied for the route request message has a path to destination or not.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

i. If next hop confirms that replying node has path, then node_id and seq_no. is stored in RREP_table.
ii. Else node_id and seq_no. is stored in malicious_table.

Step D: Once the running time (RT) is greater than waiting time (WT) all verifications are done of route reply messages.

Now select one seq_no. from the RREP_table.

While (End of RREP_table is not reached) do two step verification.

i. Compare the selected seq_no. with all other seq_no. which are present on the RREP_table, if seq_no. is exceptionally high than do next step verification and go to step D (ii).

ii. In this, the value of packet drop is checked here, if it is greater than 0.5 then store that node_id in malicious_table otherwise node_id keep in RREP_table and go to step E.

Step E: Once the all seq_no. are verified then select one highest seq_no. from the RREP_table.

While (End of RREP_table is not reached), find the cluster head.

i. Find the final weight of node using speed of link (SL), energy of link (EL) and neighborhood links (NL) and distance_time value which is getting from dt_table.

Final weight of node = (F1 * SL) + (F2 * EL) + (F3 * NL) + distance_time value.

$SL = \frac{S_a + S_b}{2}$, $EL = \frac{E_a + E_b}{2}$

a and b are two connected nodes. S_a and S_b are their speed.

E_a And E_b is the consumed energy by two nodes.

E_a is the energy of node A and E_b is the energy of node B.

F1, F2, F3 are weight factors.

F1 + F2 + F3 = 1.

ii. Then find the battery power (BP), buffer length (BL) and serve time (ST) and go to step F.

Step F: Find the node value by adding the final weight of node and all the components of step E (ii).

Node value = Final weight of node + BP + BL + ST.

And store the node value in node_value_table.

Step G: Select one highest node value from the node_value_table and make that node cluster head then send the packets to that cluster head. Cluster head will select from neighbor nodes of the sender.

Step H: Delete all other seq_no. from RREP_table.

IV. SIMULATION-BASED IMPLEMENTATION AND EXPERIMENTAL RESULTS

In this section of paper, implementation and results for HSCT are tested in mobile adhoc network environment constructed in NS-2.35. These results show effectiveness of the proposed technique. The parameters used for simulation are shown in Table 1.

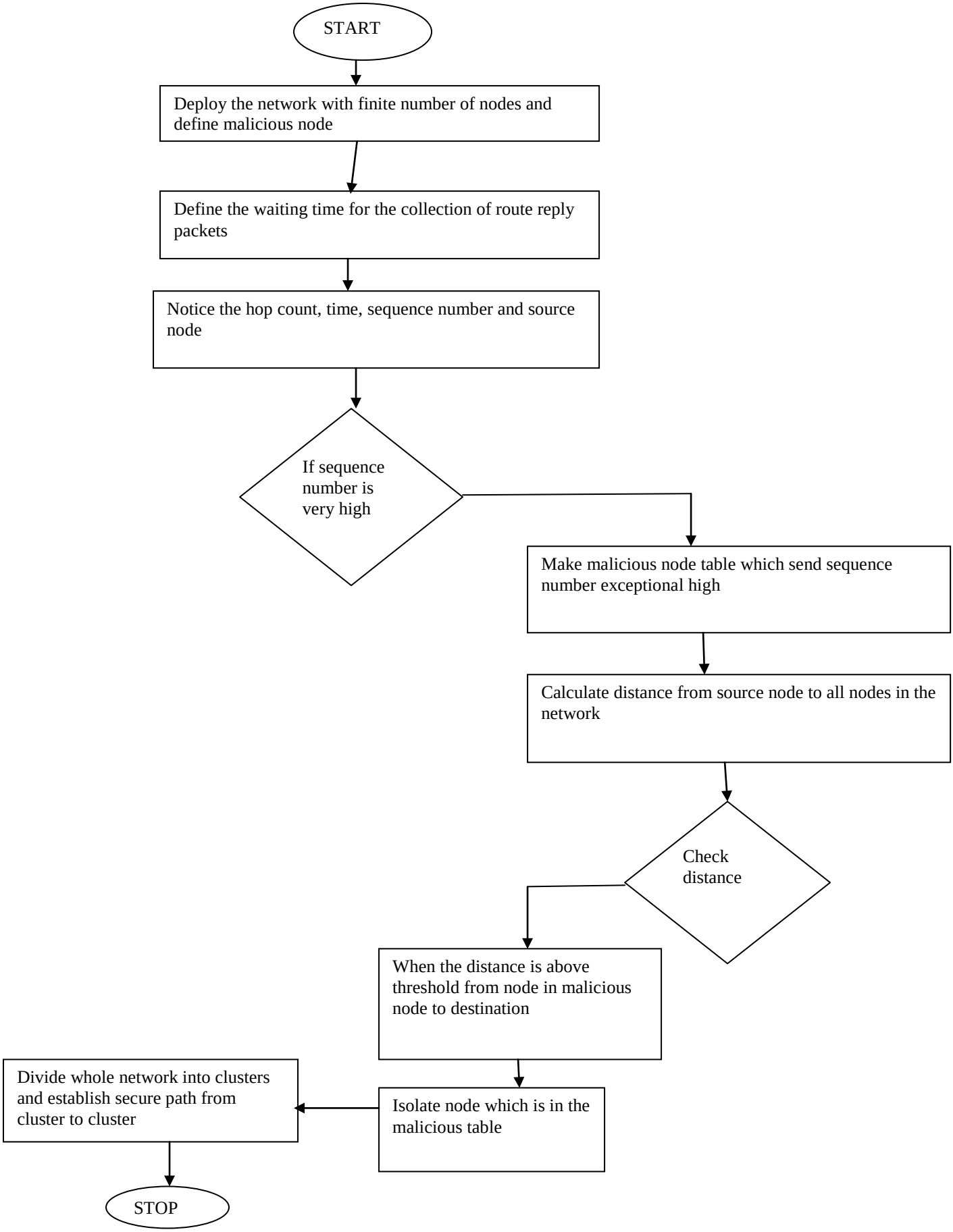
Parameter	Value
Simulator used	NS 2.3
Simulation duration	140 sec
Area (meter)	800X800
No. of nodes	15
Routing Protocol	AODV
Channel Type	Wireless
Packet Size	512 bytes
Mobility Model	Two ray ground propagation model

Table 1: Simulation parameters

After implementation of HSCT for isolation of black hole attacker nodes, a secure path from source to destination is established as shown in the figure 4.After implementing the HSCT in MANET under the attack of black hole attacker node, a secured path is obtained and performance of Adhoc networks is increased in the terms of various parameters as shown in the Figure 5, Figure 6, Figure 7 and Figure 8.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

B. FLOWCHART



CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

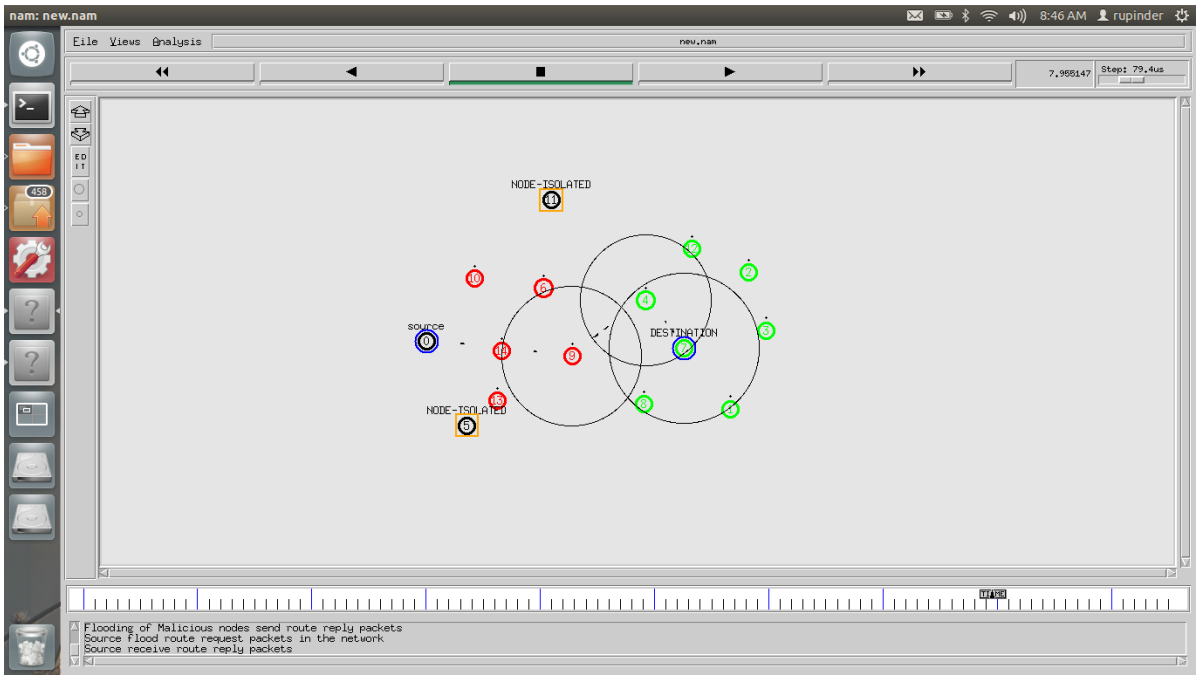


Fig. 4: Secure path from source to destination in MANET

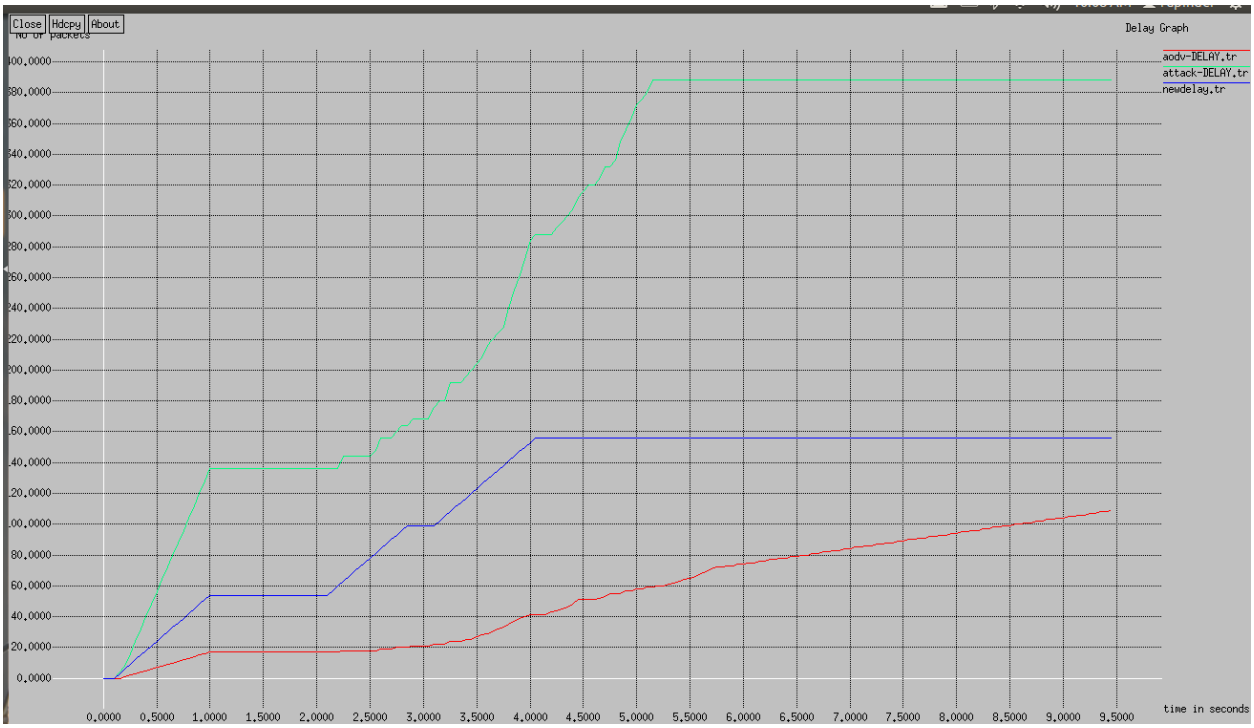


Fig. 5: Enhanced performance of HSCT in terms of Delay

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

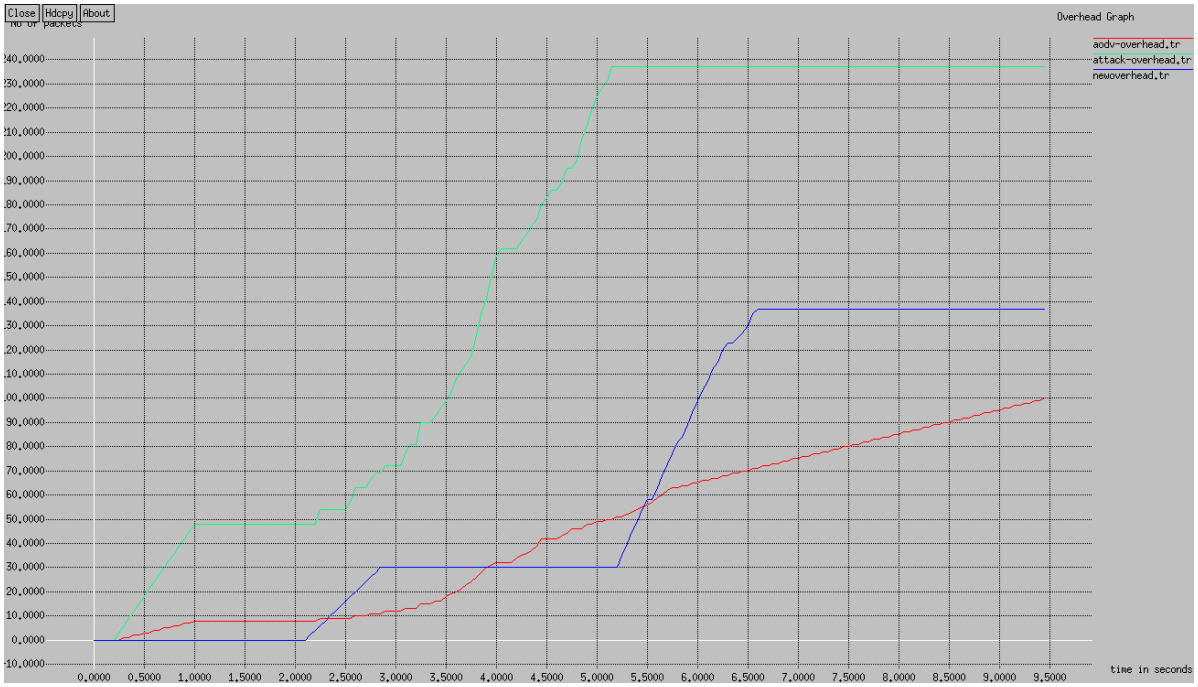


Fig. 6: Enhanced performance of HSCT in terms of Overhead

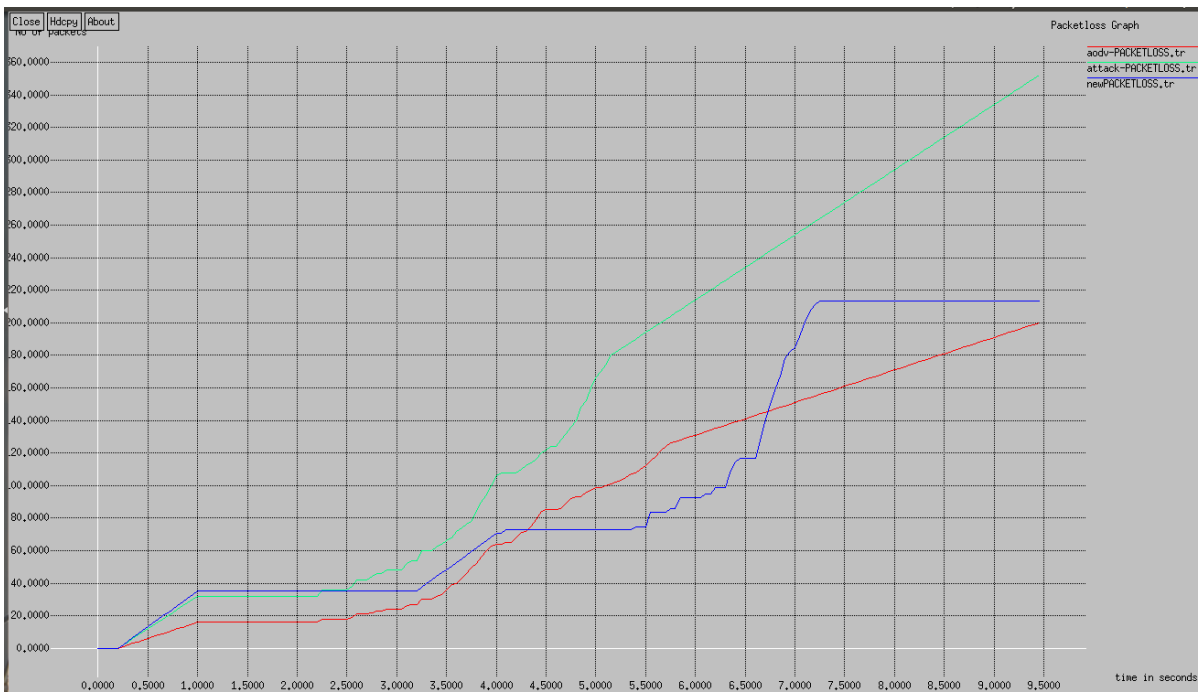


Fig. 7: Enhanced performance of HSCT in terms of Packet loss

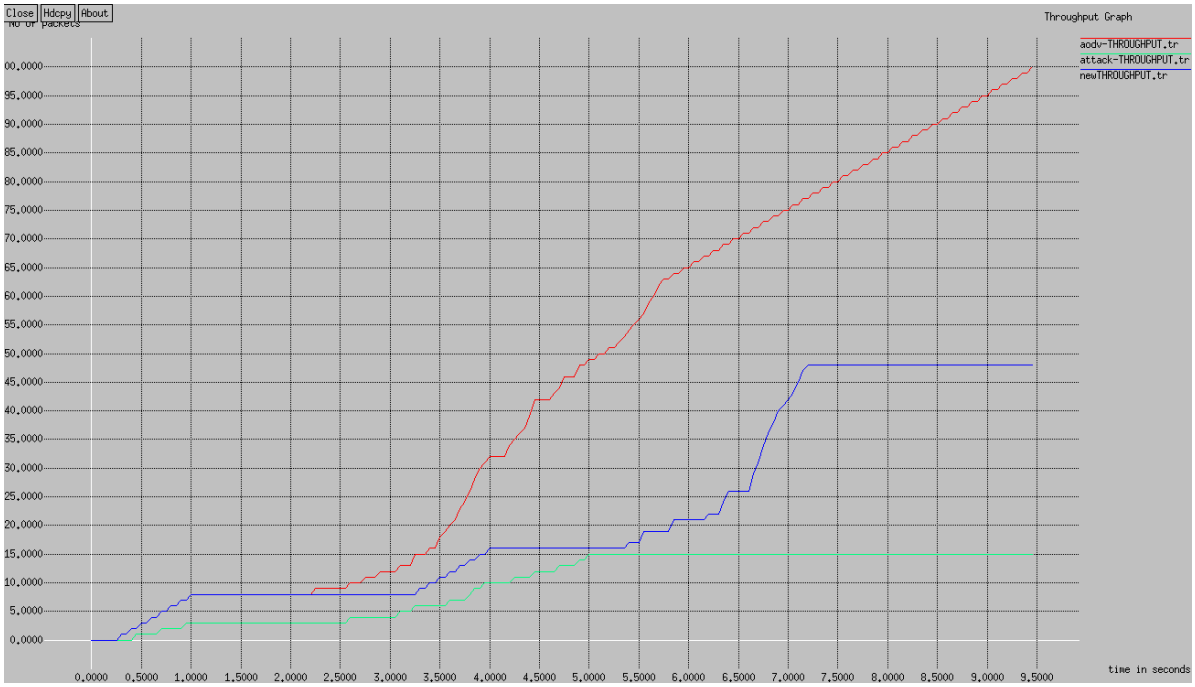


Fig. 8: Enhanced performance of HSCT in terms of Throughput

V.CONCLUSION AND FUTURE WORKS

Black hole attacks can be easily launched in mobile adhoc networks with implementing legitimacy and confidentiality. As far as security of MANETs is concern detection and prevention from black hole attack is a critical issue. In this paper, we proposed the Hybrid and Secure Clustering Technique for detection of Black hole Attack in Mobile Adhoc Networks. The proposed technique is based on detecting the black hole attack node based on minimum route reply time, minimum hop count and maximum sequence number. After detecting and isolating the malicious node from the network, concept of clustering is used for reducing the overhead. The HSCT ensures that black hole attacker node will not be left untraced in the mobile adhoc network. We have investigated the performance of our technique by using ns2 simulator. The simulation results show that our proposed technique show high performance against various parameters like packet loss, overhead, delay and throughput. In future, this proposed work can be extended by increasing number of mobile nodes in MANET to check effectiveness of proposed method. This simulation can also be enhanced for isolating some other types of attacker nodes.

ACKNOWLEDGEMENT

Authors are highly thankful to the Department of RIC, IKG Punjab Technical University, Kapurthala, Punjab, India for providing opportunity to conduct this research work.

REFERENCES

[1] Deng, H; Li, W; and Dharma, P. Routing Security in Wireless Ad Hoc Networks. IEEE Communications Magazine. October, 2002.

[2] Penga, M.; Shia, W.; Corriveaub, J.; Richard, P.; Wang, Y. Black Hole Search in Computer Networks: State-of-the-Art, Challenges and Future Directions. Journal of Parallel and Distributed Computing. June 16, 2015.

[3] Singh, J.; Kaur, L.; Gupta, S. A Cross-Layer Based Intrusion Detection Technique for Wireless Networks. International Arab Journal of Information Technology. Volume 9, No. 3, May 2012, ISSN: 1683-3198.

[4] Hsun, F.; seng1, T.; Chou1, L.; Chao, H.A survey of black hole attacks in wireless mobile ad hoc networks. a springer open journal. Human-centric Computing and Information Sciences. 2011, 1:4.

[5] Banerjee, S.; Majumder, K. A Survey of Blackhole Attacks and Countermeasures in Wireless Mobile Ad-hoc Networks. Springer. Volume 335, of the series Communications in Computer and Information Science. pp 396-407.

[6] Anand, A.; Bhandari, A. Prevention of Black hole Attack on AODV in MANET using hash function. Proceeding of 3rd international conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions). 2014.

[7] Roy, D.; Chaki, R. MCBHIDS: Modified Layered Cluster Based Algorithm for Black Hole IDS. Annual IEEE India Conference (INDICON). 2013.

[8] Jaisankar, N.; Saravanan, R.; Swamy, K. A Novel Security Approach for Detecting Black Hole Attack in MANET. Communications in Computer and Information Science. Vol. 70, pp 217-223.

[9] Banerjee, S.; Sardar, M.; Majumder, K. AODV Based Black-Hole Attack Mitigation in MANET. Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA). 2013,Volume 247, of the series Advances in Intelligent Systems and Computing pp 345-352.

[10] Rachh, A.; Shukla, Y.; Rohit, T. A Novel Approach for Detection of Blackhole Attacks. IOSR Journal of Computer Engineering (IOSR-JCE). Volume 16, Issue 2, Ver. V (Mar-Apr. 2014), PP 69-74.

[11] Dasgupta, M.; Santra, D.; Choudhury, S. Network Modeling of a Black hole Prevention mechanism in MANET. 4th IEEE International Conference on computational intelligence and communication networks. pp. 734-738, November 2012.
[12] Kurosawa, S.; Nakayama, H.; Kato, N.; jamalipour, A.; Nemoto, Y. Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method. International Journal of Network Security. Vol. 5(3): 338-346, November 2007.
[13] Jain, S.; Jain, M.; Kandwal, H. Advanced algorithm for detection and prevention of cooperative black and Grayhole attacks in mobile ad hoc networks. International journal of computer Applications. Vol. 1(7), 37–42 (2010).
[14] Sun, B.; Guan, Y.; Chen, J.; Pooch, U. Detecting Black-hole Attack in Mobile Ad Hoc Networks. IEEE conference on Personal Mobile Communications. 2003, 5th European (Conf. Publ. No. 492).
[15] Li, X.; Jia, Z.; Zhang, P.; Zhang, R.; Wang, H. Trust-based on-demand multipath routing in mobile ad hoc networks. IEEE conference proceeding, IET Information Security.Vol. 4, Issue 4, December 2010.
[16] Prachee, N.; Bhole, T. Black Hole Attack Prevention in Mobile Ad Hoc Networks using Route Caching. IEEE Conference on Wireless and Optical Communications Networks (WOCN).july 2013.
[17] Kumar, V.; Kumar, R. An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network. International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014). Bhubaneswar, Odisha, India.
[18] Bhosle, A.; Thosar, T.; Mehatre, S. Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET. International Journal of Computer Science, Engineering and Applications (IJCSEA). Vol.2, No.1, February 2012.
[19] Namdeo, M.; Patheja, P. Denial of Service (DoS) and Black Hole Attack Prevention by Enhanced Watchdog Technique in MANET. International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 5, Issue 12, December 2015.
[20] Muhammad, I.; Khan, A.; Haider, A.; Mohsin, I. Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks. Springer, Ad-hoc Networks and Wireless. Vol. 8629, pp 111-122.
[21] Chatterjee, R.; Routray, M. Black Hole Combat Using Node Stability System in MANET. Social Informatics and Telecommunications Engineering. Vol. 62, pp 249-254.
[22] Ghathwan, K.; Yaakub, A. An Artificial Intelligence Technique for Prevent Black Hole Attacks in MANET. SCDM 2014, Advances in Intelligent Systems and Computing. Springer International Publishing Switzerland 2014.
[23] Rajesh, M.; Usha, G. A Novel Honeypot Based Detection and Isolation Approach (NHBADI) to Detect and Isolate Black Hole Attacks in MANET. Wireless Personal Communication. Springer, New York 2016.
[24] Kamatchi, V.; Mukesh, R.; Kumar, R. Securing Data from Black Hole Attack Using AODV Routing for Mobile Ad Hoc Networks. Advances in Computing & Inform. Technology. Springer-Verlag Berlin Heidelberg 2013, AISC 177, pp. 365–373.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)