International Journal of Engineering & Technology, 7 (2.6) (2018) 135-140

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Energy aware detection and prevention of black hole attack in MANET

Niranjan Panda[1]*, Binod Kumar Pattanayak[2]

[1]Department of Computer Science & Engineering, S'O' A
[2]Department of Computer Science & Engineering, S'O'A
**Corresponding author E-mail: niranjanpanda@soa.ac.in*

Abstract

Energy and security are the two vital components of Mobile Ad-hoc Networks (MANETs). During routing finding an optimal path from sender to receiver sense of path length (number of hops), longevity (battery life) and security becomes an essential requirement. Variety of schemes are proposed by the researchers for finding the shortest path along with energy saving and protecting from attacks Black-hole and gray-hole attacks are some of the most harmful attacks against MANET communication and needs attention. These attacks may cause by insider or outsider malicious node(s) who may drop packets or misroute the information during communication from sender node to receiver node. In our study we proposed an intelligent routing protocol based on Ant Colony Optimization (ACO) technique that finds shortest path from source to destination, applies the concept of power aware techniques to save energy increasing the longevity of the link avoiding link failure and also uses the concept of digital signatures, watchdog and path rater for detection and avoidance ofblack-hole and gray-hole attacks. Simulation study of the proposed scheme is made over some network parameters and found to be efficient in comparison to the basic AODV routing protocol.

Keywords: *Ant Colony Optimization;Black-hole and gray-hole attack; digital signatures; intelligent routing protocol; MANET; watchdog and path rater.*

1. Introduction

Mobile Ad-Hoc Networks (MANETs) are independent deconcentrated systems or wireless systems. In the network system, MANETs always comprises of the mobile nodes which may be structures or subsystems, acting both as a router and a host. Mobile nodes within the network, depending on each other's connection they can form different network configuration or topography by their self-arrangement power, without any fixed infrastructure. Routing protocols are the most fascinating, ambitious and challenging areas in MANET research. Researchers designed a number of routing protocols for MANETs such as AODV, DSR, DSDV, OLSR etc. The very intensive worry for the basic functionality in MANET is energy saving and routing security. MANET nodes are battery powered and during routing battery life extension is one of the measure issues in them. Finding a shortest path during routing results in quicker depletion of battery life of participating nodes.Due to the characteristics such as open access medium, firmly altering network topology, deficiency of intermedial management and monitoring systems, cooperative algorithms and deficiency of transparent defense mechanism of MANETs often ill used by attackers and endure security attacks. The network services accessibility, data integrity and confidentiality can be gained by safeguarding the security problems that have been detected within the network. Moreover, the wireless connection makes MANETs to be more susceptible to the attacks by providing access to on-going communications. Varieties of attacks are found out in the MANETs and classified as; worm-hole attack, black-hole attack, rushing attack, byzantine attack, resource consumption attack, location disclosure attack, sybil attack, flooding attack, Denial of Service (DoS), spoofing attack etc. [1].

Much energy aware routing schemes [2-8] are proposed in the literature. The Minimum Total Transmission Power Routing (MTPR) [2] computes the overallenergy needed for transmitting the packets through various paths and finally chooses the one with minimum power required but the remaining power with nodes is not taken into consideration, which may lead to destruction of some nodes in the path resulting in path failure. Min-Max Battery Cost Routing (MMBCR) [3] computes the energy of each node in a path and selects the minimum power nodes in each path. Then the path having the node with maximum battery power among these minimum powered nodes is selected. MMBCR extends lifetime of a network by choosing remainingenergy of a node but neglects the consumption factor and total transmission energy. The Conditional Max-Min Battery Capacity Routing (CMMBCR) [4] combine the factors total transmission energy and remaining energy of nodes under consideration. MTPR is applicable when all the participating nodes are above the threshold value fixed for battery protection, otherwise MMBCR is used. Minimum Drain Rate (MDR) [5] uses a metric drain rate which is computed for a node as a ratio of remaining energy and rate of energy consumption considering the ongoing traffic conditions. The path with minimum drain rate and minimum battery power is chosen.

Antecedently, many more works are performed on issues of security. Black-hole attack is one of the most vulnerable type of attack which is deeply related to reactive routing protocols in MANET like AODV and DSR. In our work we condense or concentrate our study on the Blackhole attack and one of its special case known as gray-hole attack. We have proposed anenergy aware solution for detection and avoidance of black-hole and grey-hole attacks on

MANETs. The proposed scheme is analyzed and compared with basic AODV routing protocol through a simulation carried out using NS-2. Its consequences are explained by expressing the effect of this attack to interrupt the normal execution of MANET routing protocols.
In chapter 2 we discussed about the black-hole and grey-hole attacks in MANETs in details. In chapter 3 we have reviewed some of the recent works carried out for the detection of black-hole and gray-hole attack. In chapter 4 we have presented our energy aware approach for detection and avoidance ofblack-holeand gray-holeattack in MANET. Chapter5 presents the simulation study, performance metrics, analysis and comparison of proposed black-holedetection scheme withthe basic AODV routing protocol and finally in Chapter 6 we discussed about future research directions and concluded our work.

2. Black-hole attack and gray-hole attack

In black-hole attack [9] attacker nodes exploit the susceptibilityduring route discovery process of reactive routing protocols and inject false route to the destination. On receiving a RRER message intermediate attacker node replies with a RREP havinganexcessive destination sequence number than the RREQ message received claiming to the destination. When an attacker chooses the concept of rushing along with high power transmission to make this attack. It is quite impossible to find out a route not passing through the attacker node. Once the node chosen as an intermediate node or becoming part of routes in the network starts misusing or discarding the traffic being directedby it building a black-hole. This situationturns severe when the attacker becomes the part of more number of routes.
Classification of black-hole attacks made according to the presence of attacker nodessuch as:

i) Internal black-holeattack
ii) External black-holeattack

Similarly classification of black-hole attacks can be done in another way based upon the collaboration among the attacker nodes such as:

i) Single black-hole attack
ii) Collaborative black-hole attack

Gray-hole attack [10] is one of the selective dropping attacks and can be described as a special case of black-hole attack in which an attacker node becomes part of route in the network as in black-hole attack but does not drop the data packets routed through it entirely. Initially attacker node may behave as legitimate node to trust but later drop packets selectively with certain probability from some specific nodes or in some other specific pattern. In this type of attack detection of attacker nodes are very difficult as these nodes drop packets routed through them for some time whereas may behave normally as legitimate nodes for the rest of time.

2.1. Internal black-hole attack

To launch this type of attack an insider compromised node staysacross the sender and receiver nodes, becomes the part of an active route and conducts the attack. Internal black-hole attacks are named so as the attacker node by self is a member of the current network in which data transmission is carried out. This type of attacks is more endangered to guard against as it is so difficult to detect the internal compromised nodes.

2.1. Externalblack-hole attack

In this type of black-hole attack attackers remain exterior to the current network and decline access to the network traffic, disrupting the network or creating congestions as shown in Figure. Further the external black-hole attacks may lead to internal black-hole attack by compromising some of the internal legitimate nodes involving them in attacking other nodes in MANET.

2.3. Single black-hole attack

In this type of attack situations, a particular attacker node broadcasts itself for containing fresh routes towards the destination node following the shortest path and it helps the attacker node to reply all the RREQs being the part of route, further during data transfer intercepts the data packets and retaining it [11]. In reactive routing protocols that uses flooding mechanism a mischievous and forged route is created as the attacker nodes RREP is received before the legitimate ones. Being the part of route, the attacker node behaves to drop all the packets received or to send them for an arbitrary address [12]. Overall, we can say that to make a black-hole attack the attacker node becomes the part of the route but how it is not specified as it differs from protocol to protocol. In Fig. 1,shows the process of route discovery initiated by the protocol from “S” to “D” where “S” is the source node and“D” is the destination node and “A”, “C”,“E” are the intermediate nodes. Considering “B” as an attacker node and claims to have active routes to the destination “D”, on receiving RREQ packets “B” sends a RREP to “S” before other legitimate nodes making “S” to trust that “B” is a genuine node and can be a part of the active route. Hence all other RREPs from legitimate nodes are discarded by “S” and making the route discovery come to an end. Onwards “S” sends the data packets through node “B” which may be dropped or fabricated by “B” leading to a black-hole attack.

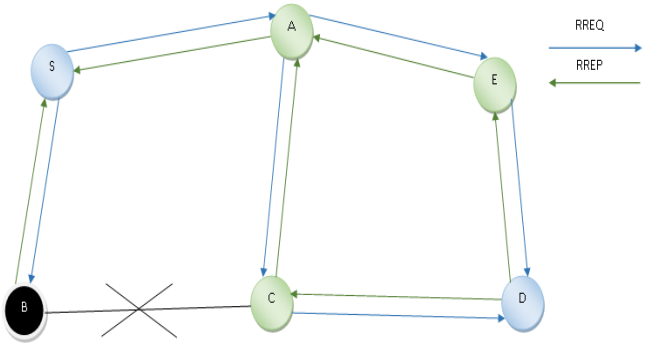

Fig. 1: Single black-hole Attack.

2.4. Cooperative black-hole attack

Some attackers perform in a classto launch this type of black-hole attacks. In Fig. 2, “S” and “D” represents the sender and receiver node respectively, nodes “A”, “B1”, “B2”, “C”, “E”, and “F” are the intermediate nodes. Considering “B1” and “B2” be the cooperative Black-hole nodes, when “S” want a data transmission to “D”, a route discovery is initiated by sending RREQ packets towardsits neighbors. The attackers will also accept the RREQ and send the RREP to “S” immediately. The RREP from “B1” reaches first at “S” before any other nodes RREP. Hence source ode “S” starts sending packets to “B1” assuming it to be legitimate node. Attacker node “B1” instead of forwarding the data packets drops them or transmitted to the other attacker node “B2”. Further “B2” drops the entire packets instead of forwarding it to towards destination.

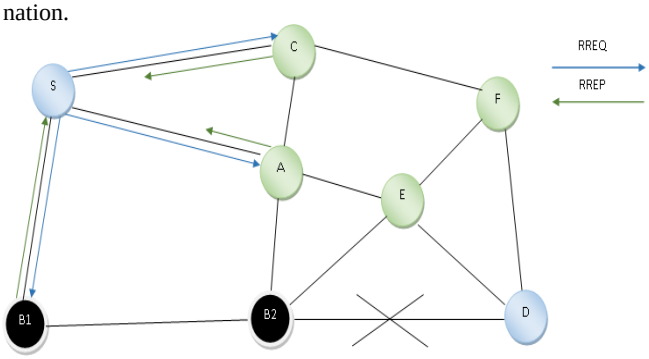

Fig. 2: Cooperative black-hole Attack.

According to [13], in the Fig. 2, when the “S” sends a ``Further Request (FRq)" to “B2” following another routing path (S-A-B2) other than the routing path through “B1” and asks “B2” for having any routing path to “B1” and “D”. As “B2” is working in cooperation with “B1”, its “Further Reply (FRp)” given positively i.e. “yes” to both the questions. Hence as suggested in [14], node Ssends data packet considering path (S-B1-B2) to beinvulnerable. Butactually, the data are dropped by the node “B1” or “B2” compromising the network security.

3. Related works

Black-hole attack is a measure security attack during routing and it needs a lot of attention to deal with this issue. Researchers proposed various security solutions to deal with this attack, but our study includes some of them based on the works carried out within these recent years.

VishvasKshirsagar et al. [15] proposed a solution to avoid packet dropping by anode using Bayes’ Theorem and Prior probability method. When a node found to drop packets, it is eliminated from the network. Using this heuristic mathematical model secure routing can be possible using an independent environment.

GayatriWahane et al. [16] put forward a mechanism for detection of cooperative black-hole attack based upon crosschecking with a timer-based mechanism called TrueLink in AODV routing protocol. Authors also conducted a simulation to prove the minimum routing overhead, delay and maximum throughput with increase in attacker nodes and pause time.

Ayesha Siddiqua et al. [17] suggested a method for detection and prevention of the black-hole attack based on secure knowledge algorithm. The authors monitored the data delivered to receiver and analyzed the reasons for packet drops during communication based upon which a node declared to be malicious as a black-hole node.

Nidhi Choudhary et al. [18] presenteda trust-based mechanism for identifying the black-hole node. A blacklist table is maintained at every node and trust value of its neighbor nodes is recorded. Trust value of any neighbor getting down the previously set threshold value, the neighbor node are indexed in the blacklist table maintained.

Ali Dorri et al. [19] suggested a detection method for black-hole attack in which next hop and previous hop node of a RREP packet is checked for the identification of misbehaving nodes in the path. Sener node identifies a misbehaving node by looking into the Data Routing Information table maintained by it.

J.M. Chang et al. [20] put forward a bait detection approach for defending against the collaborative attacks made by the malicious nodes in MANETs. Black-hole attacks are detected and prevented by designing a Cooperative Bait Detection Scheme (CBDS) which provides the benefits of proactive defense architectures as well as reactive defense architectures using a reverse tracing technique.

Abdelshafy et al. [21]presented a method to detect malicious nodes by using a concept of Self-Protocol Trustiness (SPT) and another method for resisting the black-hole attacks as Black-hole Resisting Mechanism (BRM) which can be embedded with any of the reactive routing protocols. The proposed methods use local timers and fixed threshold values for classifying any node as malicious. Simulation studies are made using NS-2 by the authors to show that the performance of the network increases by his proposed work in comparison to AODV and SAODV under black-hole attacks.

Dixit et al. [22] suggested an intrusion detection systembased onvoting todetectblack-hole attack and gray-hole attack in MANET. A routing table is maintained based on the votes made by the nodes participating within the network based on the behaviour of their neighbour nodes. Nodes with higher vote numbers create the path for routing whereas negative voting makes a node out from an active route.

4. Our proposal

Our framework uses an agent-based technique that relies on the ACO metaheuristics to find out the optimal path during routing, along with security is provided using digital signatures [23], watchdog and pathratermechanism [24] to prevent external and internal black-hole attacks respectively during communication.

Initially during network setup each mobile node registers itself with the network and assigned a private key, shared public key pair which is used by the individual mobile nodes for generation of digital signatures. Each node makes a neighbour discovery by using the HELLO messages. During communication each node selects the next hop using the metric next hop availability which can be described as a probabilistic value;

$$P_{(NH)} = (\Omega)^{\rho} / \Sigma((\Omega)^{\rho})$$

4.1. Route Discovery

Whenever a pair of nodes want to communicate with each other and no routing information is available with sender, then the source node creates a Forward Agent (FA) and attaches its own digital signature to it. Then the FA broadcasted to its neighbours. Each neighbour receiving a FA verifies its digital signature and finding it to be correct; the FA is accepted by the neighbour. Each intermediate node receiving a FA attaches its own digital signature to it and rebroadcasts to its neighbours until the destination node is reached. During its travel towards the destination, the FA's gather the path information with them.

Reaching the destination, the FA is killed and a Backward Agent (BA) is created which travels from the destination towards the source based upon the gathered information’s by the FA. BA attached with the digital signature of the destination and forwarded towards the source. Any intermediate node receiving the BA verifies the digital signature and getting it to be correct accepts the BA. BA during its travel updates the pheromone table at a node in terms of remaining energy and hop count as described in EAAR [25].

$$\Omega = MBR / H$$

Any mismatch with the verification of digital signature leads to killing the FA or BA at the middle of communication. Repeating the process at every intermediate node BAs reach the source node. Reaching the source node BA's are killed and multiple successful paths are established.

4.2. Data transfer

Once the path discovery is over and successful routes are established between the source and destination, the data transfer process starts in between them. During data transfer digital signatures are also used with all the data packets sent to provide security during communication.

4.3. Route maintenance and link failures

Source node periodically undergoes verifying the paths by sending FA's and BA's in continuous intervals of time. In between any link failure due to removal of a malicious black-hole node or any other reason may be addressed by starting a new route discovery locally from the node where no further routing information are available.

4.4. Malicious node detection

When an external attacker node wants to participate in the active route it is caught during digital signature verification phase due to the unavailability of the secret key with it, as the key is only present with the internal registered mobile nodes only. For internal misbehaving nodes, each mobile node within the network embed-

ded with a watchdog and pathrater mechanism so that they can monitor their neighbour nodes during data transfer. Every node monitors its neighbours for the factors like data packet loss, data transfer rate and false flooding etc. If any of the factors goes below the minimum threshold value, then the neighbour node put the node in the malicious node list and informs all the legitimate nodes in the network about the malicious behaviour of the node by transmitting a message.

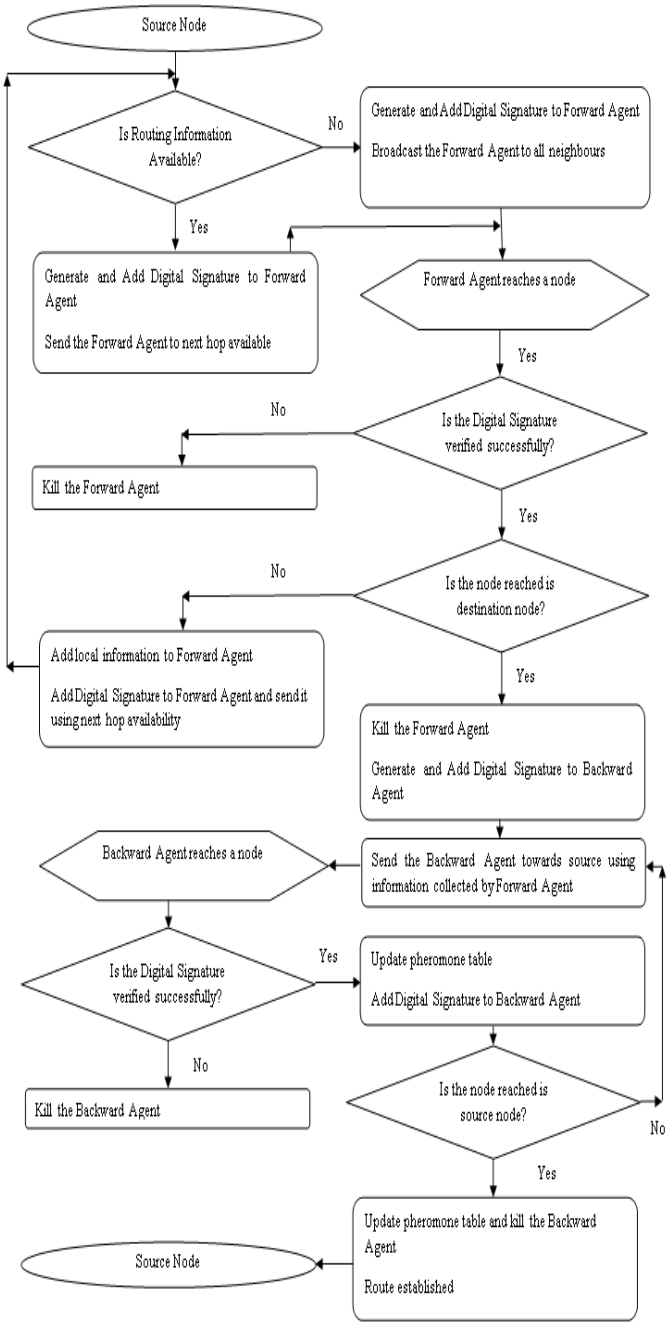

Fig. 3: Route discovery process using our proposed model.

5. Simulation and results

For the purpose of simulation modification is done to the existing AODV routing protocol according to our proposed routing methodology and compared with the basic AODV routing protocol. The simulation carried out using the network simulator NS-2.35. The view of complete simulation environment is represented in Table 1.

We have used some of the simulation parameters like packet delivery ratio and number of packets lostagainst the number of attackers.Parameters like routing overhead, network energy consumption and network throughputs are used against the simulation time for evaluation of performance of our proposed scheme in comparison to basic AODV routing protocol.

Table 1: Simulation scenario and parameter settings

Parameter Name	Value
Number of nodes	40
Node distribution	Random
Area dimension	1500 x 750
Simulation time	300 s
Propagation	Radio-propagation model
Network type	Wireless
Traffic generator	CBR
MAC type	IEEE 802.11
Data rate	11 Mbps
Antenna type	OmniAntenna
Mobility pattern	Random
Node speed	10 to 15 m/s
Interface queue type	DropTail/PriQueue
Max packet in interface queue	50

5.1. Packet delivery ratio (PDR)

PDRcan be computed asafraction of total number of data packets collected at the destination with respect to total number of packets sent by the constant bit rate (CBR) source.Performance of a network increases with the increase in packet delivery ratio values.

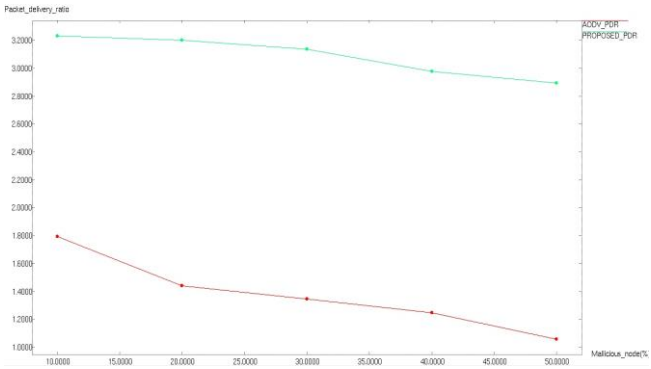

Fig. 4: Comparison graph showing packet delivery ratio.

4.2. Packet loss (PL)

PLcan be computed as a fraction of total number of packets lost due to congestion or any other reason with respect to total number of packets sent during transmission. Performance of a network increases with the decrease in packet loss values.

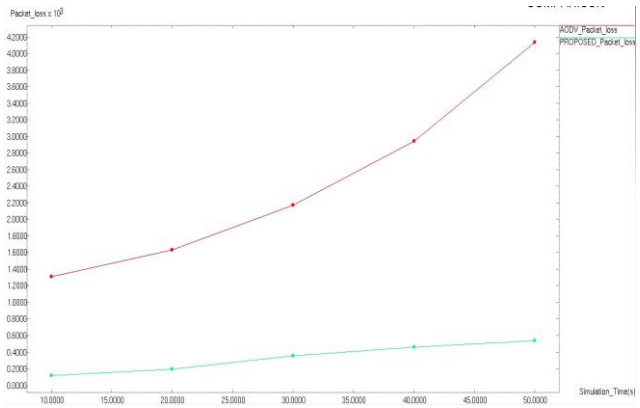

Fig. 5: Comparison graph showing number of packet lost.

4.2. Routing overhead (RO)

RO can be computedas a fraction of number of routing packet transmitted with respect to number of successfully delivered data packets where routing packets comprises control packets utilized for route discovery, route maintenance, and pheromone updates. Performance of a network increases with the decrease in routing packet overhead values.

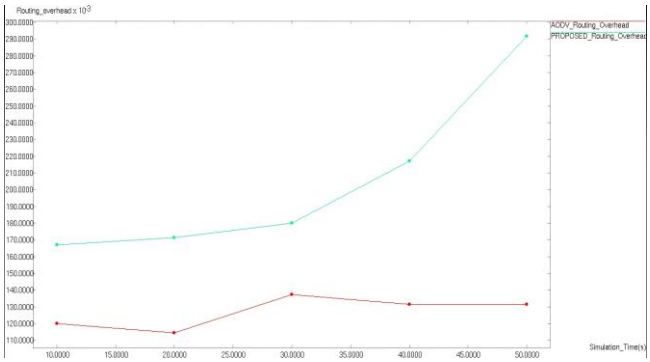

Fig. 6: Comparison graph showing routing packets overhead.

4.2. Energy consumption (EO)

EO is the part of energy spent by the nodes during receiving the packets from neighbor nodes and transmitting the packets to neighbor nodes. Performance of a network increases with the decrease in energy consumption values.

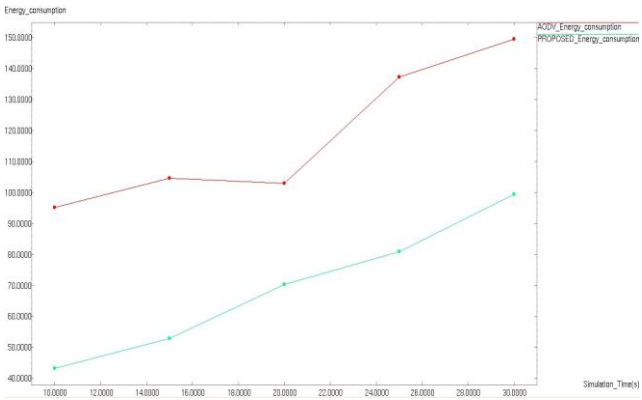

Fig. 7: Comparison graph showing average energy consumption.

4.2. Network throughput (NT)

NT can be compute as a ratio of the amount of packets moved successfully from sender to receiverwithin a particular time period and represented in bps. Performance of a network increases with the increase in throughput values.

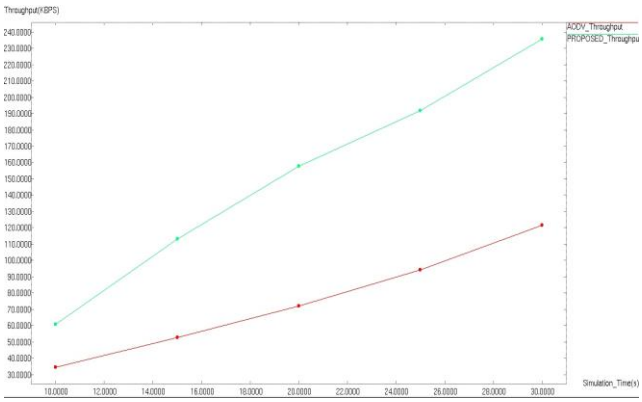

Fig. 8: Comparison graph showing network throughput.

6. Conclusion

In this article we have initialized our study with the basic idea of MANET and need of power aware secure routing features in MANET. Then we discussed about the most repeated attacks in MANET known as black-hole and gray-hole attacks. We discussed about some of the solution proposed by various researchers. A multipath intelligent routing protocol is proposed for findingan optimal path from sender to receiver along with increasing the lifetime of the network and providing securityagainst the these attacks. We analysed the effect of these attacks by simulation studies on the network parameters network routing load, network throughput, packet delivery ratio, packet loss and network energy consumption using our proposed energy aware secure routing protocol and the base AODV routing protocol. Implementations show that our proposed work detects and avoids the attacks more efficiently in comparison to basic AODV and increases network performance but increase in network routing load is also seen with increase in number of attackers.

References

[1] Pankajini Panda, Khitish Ku. Gadnayak, Niranjan Panda, “MANET Attacks and their Countermeasures: A Survey”, International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 2, no. 11, pp. 319-330, 2013.

[2] Scott, K., Bambos, N., 1996. Routing and channel assignment for low power transmission in PCS. In: Proc. Intl. Conf. Universal Personal Communications (ICUPC’96), Cambridge, MA, pp. 498–502.

[3] Singh, S., Woo, M., Raghavendra, C.S., 1998. Power-aware routing in mobile ad hocnetworks. In: Proc. 4th Annual ACM/IEEE Intl. Conf. Mobile Computing and Networking, Dallas, TX, pp. 181–190.

[4] Toh, C.-K., 2001. Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks”. IEEE Communications Magazine 39 (June (6)), 138–147.

[5] Kim, J., Garcia-Luna-Aceves, J., Obraczka, K., Cano, J.-C., Manzoni, P., 2002. Power aware routing based on the energy drain rate for mobile ad hoc networks. In: Proc. 11th Intl. Conf. Comp. Comm. Netw., pp. 565–569.

[6] Liang, W., Yuansheng, Y., 2004. Maximizing battery life routing in wireless ad hocnetworks. In: Proceedings of the 37th Hawaii International Conference on System Sciences, Hawaii, USA.

[7] Srinivas, A., Modiano, E., 2005. Finding minimum energy disjoint paths in wireless ad-hoc networks. Wireless Netw. 11, 401–417.

[8] Yuen, W.H., Sung, C.W., 2003. On energy efficiency and network connectivity of mobile ad hoc networks. In: Proc. 23rd IEEE Intl. Conf. Distrib. Comput. Sys. (ICDCS’03), Rhode Island, May 2003, pp. 38–45.

[9] Al-Shurman, Mohammad, Seong-Moo Yoo, and Seungjin Park. "Black hole attack in mobile ad hoc networks." *Proceedings of the 42nd annual Southeast regional conference*. ACM, 2004.

[10] M. Chaitanya Kishore Reddy and BoyaSripriya, “A Study on Gray-hole Attacks in Mobile Ad-hoc Networks”, 2017 International Journal of Advance Technology and Innovative Research, vol 9, pp. 1634-1636, 2017.

[11] Biswas, Kamanashis, and Md Ali. "Security threats in mobile ad hoc network." (2007).

[12] Pequeño, Guillermo Alonso, and Javier Rocha Rivera. "Extension to MAC 802.11 for performance Improvement in MANET." (2007).

[13] Perkins, Charles E., and Pravin Bhagwat. "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers." *ACM SIGCOMM computer communication review*. Vol. 24. No. 4. ACM, 1994.

[14] Deng, Hongmei, Wei Li, and Dharma P. Agrawal. "Routing security in wireless ad hoc networks." *IEEE Communications magazine* 40.10 (2002): 70-75.

[15] VishvasKshirsagar, Ashok M. Kanthe, and Dina Simunic “Analytical approach towards packet drop attacks in mobile ad-hoc networks,” IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), IEEE, 2014.

[16] GayatriWahane, Ashok M. Kanthe, and Dina Simunic, “Detection of cooperative black hole attack using crosschecking with

truelink in MANET," International Conference on. Computational Intelligence and Computing Research (ICCIC), IEEE, 2014.
[17] Ayesha Siddiqua, Kotari Sridevi, and Arshad Ahmad Khan Mohammed, "Preventing black hole attacks in MANETs using secure knowledge algorithm," International Conference on Signal Processing and Communication Engineering Systems (SPACES), IEEE, 2015.
[18] Nidhi Choudhary, and Lokesh Tharani, "Preventing black hole attack in AODV using timer-based detection mechanism," International conference on Signal processing and communication engineering systems (SPACES), IEEE, 2015.
[19] Ali Dorri and HamedNikdel, "A new approach for detecting and eliminating cooperative black hole nodes in MANET," 7th Conference on Information and Knowledge Technology (IKT), IEEE, 2015.
[20] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, HanChieh Chao, and Chin-Feng Lai, Member, IEEE "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait" (2015)
[21] M. A. Abdelshafy and P. J. B. King, "Resisting blackhole attacks on MANETs," 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, 2016, pp. 1048-1053.
[22] S. Dixit, P. Pathak and S. Gupta, "A novel approch for gray hole and black hole detection and prevention," 2016 Symposium on Colossal Data Analysis and Net-working (CDAN), Indore, 2016, pp. 1-6.
[23] Harn, Lein, Manish Mehta, and Wen-Jung Hsin. "Integrating Diffie-Hellman key exchange into the digital signature algorithm (DSA)." *IEEE Communications Letters* 8.3 (2004): 198-200.
[24] Marti, Sergio, et al. "Mitigating routing misbehavior in mobile ad hoc networks." *Proceedings of the 6th annual international conference on Mobile computing and networking*. ACM, 2000.
[25] Misra, Sudip, et al. "An ant swarm-inspired energy-aware routing protocol for wireless ad-hoc networks." *Journal of systems and software* 83.11 (2010): 2188-2199.