Improvement in QoS and Detection of Malicious node in MANET

Swati Arya[1], Tamanna[2]
Computer Science Department,
N.C. College of Engineering,
Israna, India[1,2]

***Abstract*— MANET is Mobile Adhoc Network. Mobile ad hoc networks (MANETs) are self-configured networks which do not have need of any centralized base station for monitoring and controlling the network. There is no central control in MANET. Routing is a difficult task in network as topology changes frequently. In this paper, we discuss various attacks and different types of methods to detect and respond to the collaborative attacks. QoS parameters are also used for resource utilization. Main focus in this paper is to detect the destination node whether it is malicious or not and find the stable path from source to destination. In this paper new fitness function along with hybrid of hill climbing and genetic algorithm is proposed and use collaborative attacks approach.**

Index Terms*— Mobile Adhoc Network (MANET), Quality of Services (QoS), Collaborative attacks

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are self-configured networks which do not have need of any centralized base station for monitoring and controlling the network. Topology of such networks is dynamic and the density of nodes in the network keeps changing. There is no restriction on the entry or exit of nodes to and from the MANET. Since the nodes are free to move, there is a risk of presence of intrusion by malicious nodes in the network. Nodes have limited bandwidth and limited power. They operate with the help of battery or a power source which is limited. The constraints of power and limited frequency range of MANETs are some of the issues of these networks. Other issue which is of our major concern is security for MANETs. Intrusion in a MANET can result in
problems like dropping of data packets, delay in the service, inefficiency, and decrease in throughput and increase in overhead. A node which is either malicious or has limited battery power can act selfish. Such nodes results in poor performance of the network. [1] There are several types of attacks in MANETs. They can be further categorized into
attacks depending on which layer the attack has occurred (like network layer attacks), number of nodes attacked and helped for attack (collaborative attacks), active attacks and passive attacks. Several intrusion detection techniques have been developed. These techniques not only detect the attack in the network but also provide the remedies to deal with the attack. In order to make a MANET scalable, it is crucial that there must be some intrusion detection technique combined with the routing protocol. [2] For MANETs, there are different types of routing protocols but they lack in providing security. Existing routing protocols for MANETs do not have any mechanism to check whether a node promising route to the destination is malicious or not. They rely on trustworthiness of each node in the network. All they do is choose a route that seems best at the moment either by considering the number of hops required to send the packet to the destination or by considering the early reply received by the sender node. One such routing protocol for MANETs is Dynamic Source Routing (DSR) protocol. In our thesis DSR is taken as a base protocol for routing packets in the network. It is of two types that is close and open MANET. Close MANET does not provide different types of networks to communicate with each other so it is homogenous MANET and Open MANET provide different networks to communicate with each other and they are called as heterogeneous MANET. MANET is used in many areas like spying, vehicular networking, law enforcement, rescue missions, battlefield communications and many more.
There are many QoS routing algorithm that have been proposed so far. Most of them are based on demand routing. Routes that stay for longer period of time reduce the possibility of route breaks. Due to link failure packets can be lost. Route between source to destination is better known with the help of QoS routing and also QoS requirements are satisfied. Providing QoS in Adhoc network is difficult as among adjacent nodes bandwidth is shared with them. There are many heuristic approaches that are used to find feasible path. Genetic algorithm is one of them. The process of natural selection is done with the help of genetic algorithm. It is the searching heuristic as well as optimization technique. It is difficult to meet many QoS constraints together as it is a NP-complete.

In this paper we discussed about work done so far to satisfy QoS parameters and security issues. Paths are optimized using different approaches that focus on stability of path. If appropriate parameters are selected then routing performance is improved. Multiple QoS parameters are optimized. Here we deal with collaborative attacks in mobile ad hoc networks. In this main focus is on improvement of path by using proper QoS parameters and detecting malicious nodes using collaborative attacks.

II. RELATED PAPER

Anomaly detection technique is used to detect black hole attack in the technique discussed in [5]. Since the nature of nodes in a MANET is mobile, the normal state of the network is updated. There is continuous updating of the training data which is used to decide the normal state of the network. Research has been done to detect collaborative attacks which are considered as problematic to detect. Some of these works use the concept of encryption. The technique proposed by Yin et. al. in [6] uses symmetric keys and finds a safe route by avoiding black hole attack. Network is divided into groups, where each group has a leader. Inter and intra secure keys are shared among them.

Conventional routing protocols like AODV and DSR serve the purpose of routing in wireless networks but with a danger of attack. In [7], AODV is modified to detect collaborative blackhole attack. Performance evaluation shows that the throughput of the proposed work is better than the AODV algorithm. Modification is done in the terms of creating new packets like further request and further reply. These are the modified packets of route request and route reply. A data routing information table is also introduced which makes sure to keep the record whether or not the packet is transferred to the destination by an intermediate node.

Cooperative black hole attack is detected by PCBHA [8]. Nodes are assigned fidelity level on the basis of trustworthiness and their response. Nodes are declared as a black hole when its fidelity level becomes equal to zero. Routing protocols for MANET like DSR and AODV use the method of broadcasting the request for route to the destination. This results in flooding and overhead.

Wormhole attack is detected by the algorithm based on RSS (required signal strength). RSS technique or any other technique for ranging can be used to estimate distance by the nodes. Distances are estimated from the source node. Each node is assumed to be aware of its geographic location. Estimated distance is compared by the nodes with the distance mentioned in the packet. The verification process is carried out by a hypothesis testing. [9]

Nodes in a MANET have limited battery-power and bandwidth. Their frequency range is confined to a smaller area. BAIDS [10] algorithm takes care of the overhead in order to efficiently utilize the resources of the network. Distributed architecture of intrusion detection is used by the author with the help of mobile agents. These mobile agents serve the assistance to the network in terms of communication. Their work is to analyze the network and detect attacks. Mobile agent is being created by the source node with a lifetime such that it can survive until the destination is reached. The technique proposed in [11] modifies the route request packet of AODV protocol on the basis of grid positioning of nodes.

Hashing algorithm can be used to encrypt the data which is being transmitted from source to destination. The concept of hashing algorithm is used in the work proposed in [12], where a hash function encrypts the data and also detects malevolent nodes. The message digest is not so easy to decrypt so it helps to send the data in integrated form. Table 2.1 summarizes the literature study in a chronological order.

Algorithm	Year	Technique used	Applicability
HSRBH [6]	2006	Secure key cryptography	Black hole attacks are detected.
Preventing Cooperative Black Hole Attack [7]	2007	FREQ, FREP and DRI are introduced as modification to AODV.	Collaborative black hole attack detection
PCBHA [8]	2008	Fidelity Levels are assigned to nodes.	Cooperative black hole attacks are detected.
Wormhole Attack Detection Based in Distance Verification [9]	2009	RSS and hypothesis testing	Wormhole attack detection
BAIDS [10]	2012	Mobile agents are used.	Black hole attack is detected with reduced overhead.
EGBB-AODV [11]	2015	Route request packet is modified using Grid-positioning of nodes.	Reduced number of re-broadcasting of route request packets.
HMAC-SHA512 [12]	2015	Hashing algorithm is used.	Integrated data is sent and Denial of Service attack is detected

III. COLLABORATIVE ATTACK,GENETIC ALGORITHM AND HILL CLIMBING ALGORITHM

A. Collaborative Attack

When more than one node participates in an attack then the attack is called collaborative attack. Our proposed work tries to detect collaborative attack. There are various collaborative attacks in MANETs. They can be categorized into following two types:

- Direct Collaborative Attacks

Nodes which attack the network are either internal nodes or become the part of the MANET, such a attack is called direct collaborative attack. Black hole and worm hole attacks are called direct collaborative attacks. Figure 1.1 shows collaborative black hole attack in MANET. Source node broadcasts a request for route to destination. Intermediate nodes which have route to the destination will reply with the route reply packet. Malicious node also replies with the route reply packet but when the path a-b is chosen to deliver packets by the source node then the malicious node starts dropping packet instead of delivering it to the destination node. The malicious node is being helped by the other intermediate nodes to do so. Here node 1 is cooperating with

node 2. In this way collaborative black hole attack takes place and the packet delivery ratio of the network decreases. Another type of collaborative attack is wormhole attack. A misconception is created by the malicious node that it has the shortest path to the destination and a tunnel is created between two distant nodes giving a false impression of short path.

- Indirect Collaborative Attack

Example of indirect collaborative attack in MANET is sybil attack. In Sybil attack, a malicious node steals the identity of the other node in the network and shows its malevolent nature by attacking the network. It keeps changing its identity and it becomes hard to find the malicious node. [3][4] The stolen identities can be used simultaneously (Collaborative attack) or one by one. A sybil attack can also take place by creating a new identity in the network.

B. Genetic Algorithm

Genetic algorithm is the optimization technique. It is a heuristic search approach. It is based on the process of natural evolution. Random set of solutions helps in searching the solution. Fitness plays an important role in this as it is assigned with every solution. Reproduction, crossover and mutation are the genetic operators that are used to modify solutions of population. When the termination point is satisfied these operators works iteratively. Inherent parallel processing, global perspective and simplicity are the main reasons due to which genetic algorithm are use more.

Natural selection and natural genetics are the mechanisms used in genetic algorithm. It is an optimization and search algorithm. Traditional optimization methods have different approach than genetic algorithm. It works with variables coding. Traditional optimization methods use single point approach whereas in GA [18] at one time population of point is used. At the same time number of designs is processed in genetic algorithm. In each iteration number of solutions is used than single solution.

Genetic algorithm is based on the concept of Darwin's principle which is the fittest of the solution. Sciences use GA in many fields like it is applied, experimented and studied. It is used in many real time applications. It is used to find optimal parameters than other methods.

a. Selection

Selection is called as reproduction. In selection population size is kept constant and its motive is to discard bad solutions and keeps good solution. It only select best individual and others are discarded. On population the first operator applied is selection. Mating pool is formed by selecting good strings. Proportionate selection operator is most commonly used in selection in which to string fitness and probability proportional is used. There must be one cumulative probability for strings and population size is constant. Even roulette wheel is used in proportionate selection. In this approach for good solution multiple copies are generated.

b. Crossover

When some portion strings is exchanged and two solutions are selected for crossover from mating pool. There is random selection of points. Two solutions string is selected for crossover from mating pool. Randomly points are selected. Crossover is solution must be done or not depends by the probability crossover and complete freedom is given.

New string is created by exchanging from both strings the right side portion in case of single point crossover. Random site is chosen to form new string. Crossover helps to create good strings and it can be that selections of parents for crossover are not best. Parameter space is searched with the help of crossover operators.

c. Mutation

Diversity in the population is maintained in mutation. It helps to add new features in solution string. Mutation is also used for searching the optimal solution like crossover. In this 0 is changed to 1 and viva versa. Steady convergence is achieved by keeping low mutation probability. Random search is done when mutation probability is high. In solution local improvement is done with the help of mutation. After one generation is completed then mutation is done on complete population after selection and crossover.

Good string is selected using selection operator. Two good strings are combined by crossover operator. Better string is created by doing mutation. Reproduction eliminates the bad string and create good string is only expectation. New population string creation is neither tested nor guaranteed. In real world problem genetic algorithm makes fast convergence.

C. Hill Climbing Algorithm

Good outcome is achieved from hill climbing as it is based on greedy algorithm. In this single element is changed to find better solution and it is iterative algorithm. No improvement is done if better solution is not produced and process is repeated. It belongs to local search. It is based only on mutation not on crossover. In search space varying sizes jumps are taken by mutation rate. In this search is randomly and next location is selected randomly when one peak is found. Nearest extremum is achieved in hill climbing algorithm.

Local optimum is known from hill climbing algorithm but global optimum is not guaranteed. It is optimal in convex problems. It is an optimization algorithm which is used mostly because of its simplicity. It is used in real time systems and artificial intelligence. When there is time constrained it gives best result then other algorithms. Interruption in processing is done then also this algorithm gives valid result so it is known as anytime algorithm.

IV. PROPOSED ALGORITHM

If selection of best route is done by satisfying the more QoS [13] parameters then the route is more stable. So there is a need to implement a system that satisfies more QoS constraints to make the route more stable and feasible. Robustness is the main factor that must be taken in consideration and system must be optimized. To provide optimal solution for large population an algorithm must be implemented to give the optimal solution. Genetic algorithm is applied to produce optimal solution for large population. Sometimes information about the network is not complete so in this situation there must be optimal path that we get in a few iterations. So for selection of parents we applied hill climbing algorithm as hill climbing algorithm is less random then genetic algorithm. Hybrid of genetic and hill algorithm is applied to find more stable path and to reduce randomization.

Then we implement the existing approach (CBDS) to detect collaborative attacks in MANET using the MATLAB. Then with the help of various metrics such as Packet Delivery Ratio, End-to-End Delay, Routing Overhead and Throughput we will compare the protocols CBDS [14] with different thresholds, DSR and our proposed work MGBDS. Then we can analyze which approach gives better performance and under what conditions.

INPUT:
Max_I: max iterations
P_S: Population size
W_N: Worker node number

Output:
elite, W_N: Best Solution
iterator;
fit ⟵ Φ
elite1, W_N , *h1,h2,* P_S, W_N, *;*
Fit 1, P_S ⟵Φ
h 1,h2 ⟵*Hill Climbing*
while *iterator* < Max_I **do**
p_c=0.8,p_m=0.05
if *random (0,1)*<p_c **then**
temp1, W_N ⟵ *crossover(h1,h2)*
end if
if *random (0,1)*<p_m **then**
$P_{1,N}$ ⟵ *mutate(temp)*
end if
for i=1 to P_S **do**
Fit_i ⟵fitfunc (i)
end for
$elite_{1,N}$ ⟵ *best fitness value of individual*
iteratation⟵ *iteratation +1*
end while

Genetic algorithm and Hill Climbing algorithms are used in this algorithm. It helps to find stable paths and reduce randomization. In this approach QoS parameters are used along with used to find if there is any attack during the transmission of data. Many QoS parameters are used to find stable path but no approach used the QoS parameters along which can find more secure paths with stability. So this new approach is designed to find path with stability and security .

Fitness Function

Best individual in genetic algorithm [14] is known from the fitness function. Next iteration individual is selected whose fitness value is high than the previous fitness value. Requirements create the fitness value. QoS constraints are used in fitness function; these constraints contain few parameters only to calculate fitness function. So the new approach contains as many as parameters [3] to find fitness function that produce stable path. Penalty function, end-to-end delay, path loss, throughput and residual battery energy QoS constraints are used in this new approach. It helps to find more stable path if more constraints are used to find fitness function and stable routes.

$Fit_c = fit_p * fit_d * fit_{pl} * fit_t * fit_r$

where fit_c is the fitness function of complete tree. Penalty function is denoted by fit_p, End-to-End delay is denoted by fit_d, how much time is take during transmission and data loss is denoted fit_{pl} is path loss, transmission of data is denoted by fit_t is throughput and replacement the lower battery energy with the high battery energy is denoted by fit_r which is the residual battery capacity .

V. CONCLUSION

Most important requirement in mobile network is optimization. So to improve optimization we proposed a new approach that helps to find stable and secure path in the network to improve optimization. In this paper we discuss about various attacks on the MANET and techniques that are used and there applicability. More secure and stable path from destination is best known if the more QoS parameters are used to find stable paths and secure the paths from the various attacks. This is the new approach that is used to find stable as well as secure path in the MANET. There is no such way to find that is the destination is secure or it is a malicious node. So main focus of our approach is to detect the destination node whether it is malicious or not and find the stable path from source to destination. In this proposal new fitness function along with hybrid of hill climbing and genetic algorithm is proposed and use collaborative attacks approach. This new designed approach will be implemented in future.

REFERENCES

[1] Ismail, Zahian, and Rosilah Hassan. "Effects of packet size on AODV routing protocol implementation in homogeneous and heterogeneous MANET."Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on. IEEE, 2011.

[2] [illegible] vulnerabilities, challenges, attacks, application." IJCEM [illegible] Computational Engineering & Management 11 (2011): 32-37.

[3] Kundu Pooja, Neeti Kashyap, and Neha Yadav. "Literature Survey on Intrusion Detection Systems in MANETs." Information Systems Design and Intelligent Applications. Springer India, 2016. 357-366.

[4] Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao. "A survey of black hole attacks in wireless mobile ad hoc networks." Human-centric Computing and Information Sciences 1.1 (2011): 1-16.

[5] Gunasekaran, Raghul, et al. "An Improved Parallel Genetic Algorithm for Path Bandwidth Calculation in TDMA-Based Mobile Ad Hoc Networks." 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies. IEEE, 2009.

[6] Mauve, Martin, Jörg Widmer, and Hannes Hartenstein. "A survey on position-based routing in mobile ad hoc networks." Network, IEEE 15.6 (2001): 30-39.

[7] Zhong, Sheng, Jiang Chen, and Yang Richard Yang. "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks." INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies. Vol. 3. IEEE, 2003.

[8] Kurosawa, Satoshi, et al. "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method." IJ Network Security5.3 (2007): 338-346.

[9] Yin, Jian, and Sanjay Kumar Madria. "A hierarchical secure routing protocol against black hole attacks in sensor networks." Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on. Vol. 1. IEEE, 2006.

[10] Weerasinghe, Hesiri, and Huirong Fu. "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation." Future generation communication and networking (fgcn 2007). Vol. 2. IEEE, 2007.

[11] Tamilselvan, Latha, and V. Sankaranarayanan. "Prevention of co-operative black hole attack in MANET." Journal of networks 3.5 (2008): 13-20.

[12] Zhou, Yifeng, Louise Lamont, and Li Li. "Wormhole attack detection based on distance verification and the Use of hypothesis testing for wireless ad hoc networks." Military Communications Conference, 2009. MILCOM 2009. IEEE. IEEE, 2009.

[13] Asraf, Noor M., Raja N. Ainon, and Phang Keat Keong. "QoS parameter optimization using multi-objective genetic algorithm in MANETs." Mathematical/Analytical Modelling and Computer Simulation (AMS), 2010 Fourth Asia International Conference on. IEEE, 2010.

[14] Touzene, Abderezak, and Ishaq Al-Yahyai. "Performance Analysis of Grid Based AODV Routing Algorithm for AD Hoc Wireless Networks."International Journal of Communications, Network and System Sciences8.13 (2015): 523.

[15] An, Hui-Yao, et al. "A cluster-based multipath dynamic source routing in MANET." Wireless And Mobile Computing, Networking And Communications, 2005.(WiMob'2005), IEEE International Conference on. Vol. 3. IEEE, 2005.

[16] Akhter, Amina, and Teerapat Sanguankotchakorn. "Modified AODV for multi-constrained QoS routing and performance optimization in MANET." Electrical Engineering/Electronics Computer Telecommunications and Information Technology (ECTI-CON), 2010 International Conference on. IEEE, 2010.

[17] Sarma, Nityananda, and Sukumar Nandi. "Route stability based QoS routing in mobile Ad Hoc networks." Wireless Personal Communications 54.1 (2010): 203-224.

[18] Lu, Ting, and Jie Zhu. "Genetic algorithm for energy-efficient QoS multicast routing." Communications Letters, IEEE 17.1 (2013): 31-34.

[19] Chandra, ML Ravi, and P. Chandra Sekhar Reddy. "Energy Efficient QoS Routing Protocol based on Genetic Algorithm in MANET." Global Journal of Computer Science and Technology 14.7-E (2014): 9.

[20] Saha, Himadri Nath, Aparajita Chattopadhyay, and Debabrata Sarkar. "Review on intelligent routing in MANET." Computing and Communication (IEMCON), 2015 International Conference and Workshop on. IEEE, 2015.