MITIGATION OF BLACK HOLE ATTACK IN MOBILE AD-HOC NETWORK USING ARTIFICIAL INTELLIGENCE TECHNIQUE

LIKHITHA

Dept. of Computer Applications, SNGIST, Ernakulum, India

Abstract - *This research has dealt with the detection and mitigation of black hole attack in MANET. Generally, the black hole attack can be easily deployed with an adversary. It is one of the known security threats in the network. Black hole occurs because of the malicious nodes that draw the data packet with the false route. In this research, AODV routing protocol is being used. Genetic algorithm for the optimization of the route from the source to the destination has been used with the neural network that detects and prevents the network from the black hole attack. The simulation has been carried out in MATLAB environment and the performance is being calculated with the number of parameters, like, Throughput, PDR, Delay and energy consumption.*

Key Words: **Neural network, Genetic algorithm, MANET, AODV routing protocol**

1. INTRODUCTION

MANET (Mobile ad hoc network) is known as infrastructure less IP (internet protocol) network for wireless and mobile machine nodes integrated with the nodes. In the experiment, the MANET nodes do not contain a mechanism of centralized administration. MANET is considered for the routable network in which every node behaves as a router for forwarding the traffic to another particular network node.

MANET communication is consisted of two phases, route discovery and data transmission. These phases are susceptible for number of attacks. Initially, the rival might interrupt the route discovery by copying the control traffic being forged. Accordingly, the attackers may block the legitimate route control traffic propagation and wrongly manipulate the benign nodes general knowledge. Generally there are two types of attacks in the MANETs, one is Passive attack and other is Active attack.

In Passive attack, the intruder silently listen the communication channel without modifying or destroying the data packets. But in Active attack, intruder can modify or destroy the original data. Due to minimal configuration and quick deployment, MANETs are suitable for emergency situations like Natural disasters rescue operation, hospitals, battlefield, conferences and Military applications. Thus data transfer between two nodes must require security. But the active attacks like Black hole attack, Rushing attack, Wormhole attack have great impact on the performance of the network.

For providing the complete security, the discussed MANET phase communication should be guarded safe. It is to be notice that the secure routing protocols guarantee that the accuracy of the information of discovered topology cannot by itself sure the safety and the undisrupted transmitted data delivery. The approach to secure the network at the network layer is by securing the routing protocol for the prevention of probable attacks. In concise, the routing protocol task discovers the topology for ensuring that every node can obtain a recent network topology map to develop the routes.

A Vehicular Ad-Hoc Network or VANET is a sub form of Mobile Ad-Hoc Network or MANET that provides communication between vehicles and between vehicles and roadside base stations with an aim of providing efficient and safe transportation. A vehicle in VANET is considered to be an intelligent mobile node capable of communicating with its neighbors and other vehicles in the network. VANET introduces more challenges aspects as compare to MANET because of high mobility of nodes and fast topology changes in VANET. Various routing protocols have been designed and presented by researchers after considering the major challenges involved in VANETs .This paper provides a survey of routing protocols for VANET. It covers application areas, challenges and security issues prevailing in VANETs.

Vehicular Ad Hoc Networks (VANETs) is technology that integrates the capabilities of new generation wireless networks to vehicles. VANET builds a robust Ad-Hoc network between mobile vehicles and roadside units. It is a form of MANET that establishes communication among nearby vehicles and adjacent fixed apparatus, usually described as roadside apparatus.

Recently, with the development of vehicle industry and wireless communication technology, vehicular ad hoc networks are becoming one of the most promising research fields. VANETs which use vehicles as mobile nodes are a subclass of mobile ad hoc networks (MANETs) to provide communications among nearby vehicles and between vehicles and nearby roadside equipment but apparently differ from other networks by their own characteristics. Specifically, the nodes (vehicles) in VANETs are limited to road topology while moving, so if the road information is available, we are able to predict the future position of a vehicle; what is more, vehicles can afford significant computing, communication, and sensing capabilities as well as providing continuous transmission power themselves to support these functions.

However, VANETs also come with several challenging characteristics, such as potentially large scale and high mobility. Nodes in the vehicular environment are much more dynamic because most cars usually are at a very high speed and change their position constantly. The high mobility also leads to a dynamic network topology, while the links between nodes connect and disconnect very often. Besides, VANETs have a potentially large scale which can include many participants and extend over the entire road network .It is precisely because of both of these unique attractive features and challenging characteristics that VANETs could draw the attention from both industry and academia.

Therefore, several articles have tried to summarize the issues about vehicular networks. The authors discuss the research challenges of routing in VANETs and then summarize and compare the performance of routing protocols; Hartenstein and Laberteaux present an overview on the communication and networking aspects of VANETs and summarize the current state of the art at that time Raya and Hubaux address the security of VANETs comprehensively and provide a set of security protocols as well ;in the authors propose a taxonomy of a large range of mobility models available for vehicular ad hoc networks. These articles all reviewed specific research areas in VANETs. In addition, others papers like provide comprehensive overview of applications, architectures, protocols, and challenges in VANETs and especially introduce VANETs projects and standardization efforts in different regions (i.e., USA, Japan, and Europe); Al-Sultan et al. provide detailed information for readers to understand the main aspects and challenges related to VANETs, including network architecture, wireless access technologies, characteristics, applications, and simulation tools .Compared with these current articles, this paper adds the introduction of layered architecture for VANETs so that the summary of network architecture is more complete. Also, we organize the overview of the vehicular ad hoc networks in a novel way.

We introduce the VANETs from the research perspective in the paper, including some current hot research issues and general methods, which do good to the progress of VANETs. Moreover, we provide a more comprehensive analysis on VANETs research challenges and future trends, beneficial for further systematic research on VANETs. In summary, this paper covers basic architecture, some research issues, general research methods of VANETs, and some key challenges and trends as well as providing an overall reference on VANETs.

2. LITERATURE REVIEW

Rajni Garg[1] , In this research, AODV routing protocol is being used. Genetic algorithm for the optimization of the route from the source to the destination has been used with the neural network that detects and prevents the network from the black hole attack. The simulation has been carried out in MATLAB environment and the performance is being calculated with the number of parameters, like, Throughput, PDR, and Delay and energy consumption.

Mehran Abolhasan [2], The infrastructure less and the dynamic nature of these networks demands new set of networking strategies to be implemented in order to provide efficient end-to-end communication. This along with the diverse application of these networks in many different scenarios such as battlefield and disaster recovery, have seen MANETs being researched by many different organizations and institutes. MANETs employ the traditional TCP/IP structure to provide end-to-end communication between nodes. However, due to their mobility and the limited resource in wireless networks, each layer in the TCP/IP model requires redefinition or modifications to function efficiently in MANETs. One interesting research area in MANET is routing

N. K. Kuppuchamy [3], Independent, self-governing, mobile wireless hosts communicating through wireless links and forming a temporary network dynamically without centralized infrastructure are called Mobile Ad-hoc Networks (MANETs). As MANET nodes are not stationary, the same routing path may not always be taken between sender and receiver(s). Hence, such routing is complicated. Simulation results demonstrate the efficiency of the proposed hybrid fuzzy routing when compared to Ad hoc On-demand Distance Vector routing (AODV)

Iavn d chakers [4], In this paper we describe the event triggers required for AODV operation, the design possibilities and the decisions for our Ad hoc On-demand Distance Vector(AODV) routing protocol implementation, AODV-UCSB. This paper is meant to aid researchers in developing their own on-demand ad hoc routing protocols and assist users in determining the implementation design that best fits their needs.

Sina Shahabi [5], Ad Hoc network is a temporal network which is managed by autonomous nodes which have the ability to communicate with each other without having fixed network infrastructure or any central base station This algorithm tries to identify malicious nodes according to nodes' behaviors in an Ad Hoc network and delete them from routing. The suggested algorithm is simulated by NS2. The simulation results show some improvements in end-to-end delay and packet delivery rate in the suggested algorithm.

Moirangthem Marjit Singh [6], Black hole attack is a very common type of security attack found in Mobile Adhoc Network (MANET). In Black hole attack, the malicious node attracts all the data packets towards it using some false means and affects the data transmission in many ways, such as dropping of the packets. Black hole attack is vulnerable to security in MANET routing protocol.

The paper focuses to provide a snapshot on various methods of detecting black hole attack in MANET and critically eviews them. At present, several efficient routing protocols have been proposed for MANET. Most of these protocols assume a trusted and cooperative environment. However, in the presence of malicious nodes, the networks are vulnerable to various kinds of attacks.

B.kannhavong [7], recently mobile ad hoc networks became a hot research topic among researchers due to their flexibility and independence of network infrastructures, such as base stations. Due to unique characteristics, such as dynamic network topology, limited bandwidth, and limited battery power, routing in a MANET is a particularly challenging task compared to a conventional network. Early work in MANET research has mainly focused on developing an efficient routing mechanism in such a highly dynamic and resource-constrained network. At present, several efficient routing protocols have been proposed for MANET. Most of these protocols assume a trusted and cooperative environment.

3. EXISTING SYSTEM

A black hole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. One cause mentioned in research is through a denial-of-service attack on the router using a known DDoS tool. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent .Black hole attack is a special type of attack that generally occurs in the Reactive protocols. A black-hole node is the malicious node that attracts the packets by falsely claiming that it has shortest and fresh route to reach the destination, then drops the packets. These Black hole nodes may perform various harmful actions on the network that are:

- Behaves as a Source node by falsifying the Route Request packet.
- Behaves as a Destination node by falsifying the Route Reply packet.
- Decrease the number of hop count, when forwarding Route Request packet.

3.1 Disadvantages of Existing System

In the existing system the malicious node may access the data and use the data in an unauthorized way. Also hosts are specifically vulnerable to collaborative attacks where multiple hosts will become compromised and deceive the other hosts on the network. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent. The malicious router can also accomplish this attack selectively, e.g. by dropping packets for a particular network destination, at a certain time of the day, a packet every n packets or every t seconds, or a randomly selected portion of the packets. This is rather called a greyhound attack. If the malicious router attempts to drop all packets that come in, the attack can actually be discovered fairly quickly through common networking tools such as trace route. Also, when other routers notice that the compromised router is dropping all traffic, they will generally begin to remove that router from their forwarding tables and eventually no traffic will flow to the attack. However, if the malicious router begins dropping packets on a specific time period or over every n packet, it is often harder to detect because some traffic still flows across the network. The packet drop attack can be frequently deployed to attack wireless ad hoc networks. Because wireless networks have a much different architecture than that of a typical wired network, a host can broadcast that it has the shortest path towards a destination. By doing this, all traffic will be directed to the host that has been compromised, and the host is able to drop packets at will. Also over a mobile ad hoc network, hosts are specifically vulnerable to collaborative attacks where multiple hosts will become compromised and deceive the other hosts on the network.

4. PROPOSED SYSTEM

In this system we detect the malicious node that is trying to access the data using AODV routing protocol and artificial intelligence. AOMDV creates a more extensive AODV by discovering, at every route discovery process, a multipath (i.e. several other paths) between the source and the destination. AOMDV likewise offers two key services: route discovery and route maintenance. Since it greatly depends on the AODV route information, which is already available, AOMDV incurs less overhead than AODV through the discovery of multiple routes. The objective of the research is the prevention of black hole attack by utilizing the AODV routing protocol. GA (Genetic algorithm) optimization and ANN (Artificial bee colony) algorithm has been utilized for the mitigation of the black hole attack.

4.1 Advantages of Proposed System

- Security: message can’t be seen in intermediate node.
- Free from attack: Message send by attackers are not forwarded to other nodes since it affect the network lifetime.
- Increase network lifetime: Network life time will be increased by sending message only through node with high energy.
- Reliability: By “reliability” we mean the probability that a message generated at one place in the network can actually be routed to the intended destination.

5. SYSTEM DESIGN

System design refers to the description of a new system based on the information that is collected during the analysis phase and the process by which it is developed. It is the creative process of inventing and developing new inputs, database procedures and outputs to meet the system objectives. System design builds on the information gathered during system analysis. The system analyst must have a clear- cut understanding about the objectives, which the design aims to fulfill.

System Design involves translating system requirements and conceptual design into technical specifications and general flow of processing. After the system requirements have been identified, information has been gathered to verify the problem and after evaluating the existing system, a new system is proposed.

System Design is the process of planning of new system or to replace or complement an existing system .It must be thoroughly understood about the old system and determine how computers can be used to make its operations more effective.

System design sits at technical the kernel of system development. Once system requirements have been analyzed and specified system design is the first of the technical activities-design, code generation and test- that required build and verifying the software. System design is the most creative and challenging phases of the system life cycle. The term design describes the final system and the process by which it is to be developed.

System design is the high level strategy for solving the problem and building a solution. System design includes decisions about the organization of the system into subsystems, the allocation of subsystems to hardware and software components and major conceptual and policy decision that forms the framework for detailed design.

5.1 Input Design

Input design is the method by which valid data are accepted from the user. This part of the designing requires very careful attention. If the data going into the system is incorrect then the processing and output will magnify these errors. Inaccurate input data are the most common cause of errors in data processing. Input design consists of the following processes:-

- Designing graphical user entry screen is easy to use.
- Designing procedures and functions to valid the data as per business rules.
- Designing functions needed to store data into a usable form for processing.
- Designing the common integrated functions that can be used by all other users when needed.

5.2 OUTPUT DESIGN

Output design is one of the most important features of the information system. When the output is not of good quality, the users will be averse to use the newly designed system and may not use the system. There are many types of outputs, all of which can be either highly useful or can be critical to the users, depending on the manner and degree to which they aroused. Outputs from computer system are required primarily to communicate the results of processing to users. They are also used to provide a permanent hard copy of the results for later consultation.

6. BLACK HOLE ATTACK

In MANET, with AODV protocol, the black hole node assume to have fresh enough route towards the destination demanded by the nodes and takes up the network traffic. When the source node transfers the RREQ message to some destination, the black node instantly responds with RREP message with the highest sequence number and the message is taken as it is impending from the destination or from the node with the fresh towards the destination. The source node then initializes by sending the data packets to the black hole node with the trust that the packets would reach the destination.

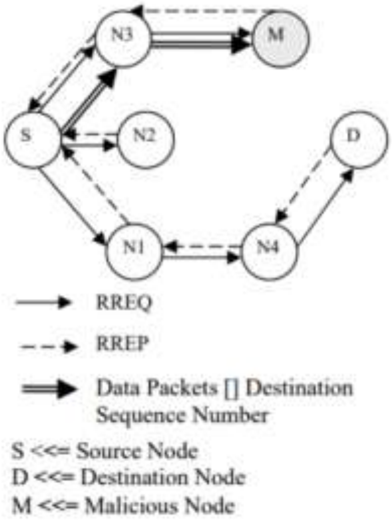

Figure 1: Black hole attack

As shown in the above figure, the destination sequence number be 32 bit integer being connected with each route and is utilized for deciding the exact route freshness. The node N3 would transfer that to the node. As the node N1 with the node N2 doesn't have the route towards the node D, it will again send the RREQ control message. RREQ control message has been send the Node N3 being expected to be taken by node M. Therefore, the node M produces the false RREP control message and transfers it to the node N3 with enhanced destination sequence number transferred to node S. Though, in AODV, as the destination sequence number is more, the route from the node would be taken be fresh and therefore, node S will start transferring the data packets to node N3.

7. ALGORITHMS

7.1 Genetic Algorithm

```
function GA ()
{
Initialize population;
Calculate fitness function;
While(fitness value != termination criteria)
{
Selection;
Crossover;
Mutation;
Calculate fitness function;
}
}
End
```

7.2 Artificial Neural Network Algorithm

```
Initialize the ANN
Net= newff (Training_data, Ggroup, Neurons)
Where, Training_data=All data
Ggroup= No. of categories
Neurons=50
Initialize the training parameters
Epoch=1000
Levenberg marquardt
Performance= MSE, gradient, mutation, & validation checks
Net= Train (Net, Training_data, Group)
Return Net as output of ANN
```

8. Simulation of Proposed work

The steps followed for the simulation of the proposed work are defined below:

1. Development of a simulator with 1000*1000 as height and width has been taken place. Firstly, n number of nodes are executed in MANET for the simulation with x as well as y co-ordinates.
2. The source and the destination are introduced with the creation of the simulator with N number of nodes with the usage of co-ordinates.
3. Coverage area is initiated with each node with source and the destination. The coverage area for the network is 20% for total network area.
4. AODV routing protocol is developed for the route discovery for source and the destination node.
5. GA algorithm is considered for route discovery and for searching the best route selection with the coverage set.
6. Fitness function has been described for GA as per network requirements.
7. When the route discovery takes place, the performance parameters are calculated and if the performance is being degraded, then the classification of the attack would be done by using NN.
8. According to attacker's activity, the attacker kind is measured and the performance of the attacker is measured to have the better results.
9. Metrics, such as, throughput, delay, energy consumption and BER are measured for checking the proposed work performance.

9. CONCLUSION

The MANET is one of the most important and essential technology that support pervasive computing scenario. The special characters of the MANET bring this technology great opportunity together with several challenges. Currently the MANET is becoming more interesting research area and many research projects employed by academic and companies all over the world. The research has analyzed and mitigated black hole attack in MANET. GA is being used for the reduction of delay, BER and for the enhancement of throughput. ANN as a classifier has been used. A variety of work has been done for the detection of black hole attack but did not utilize routing protocol for the betterment of the results. This research has used AODV routing protocol with the optimization and the classification algorithm. Parameters, like, throughput, BER, Delay and energy consumption has been utilized for the performance calculation.

10. FUTURE SCOPE

In this paper the routing security issues of MANETs are discussed and proposed solution to detect black hole attack that degrades the performance of network and drop the data packet by giving false reply about having shortest route destination node. The proposed solution can be useful in detection of black hole node and finding securing path from source to destination. As future work, we intend to develop the simulation of our proposed methodology to evaluate its performance.

REFERENCES

[1] Rajni Garg, Vikas Mongia Computer Engineering Department, Guru Nanak College, Moga, Punjab, India

[2] Mehran Abolhasan a , Tadeusz Wysocki a , Eryk Dutkie ewiczb, a Telecommunication and Information Research

Institute, University of Wollongong, Wollongong, NSW 2522, Australia b Motorola, Australia Research Center

[3] Subbaiah, K. V., & Naidu, M. M. (2010). Mobile Ad Hoc Network. Simulation, 1(04), 246-251.

[4] Royer, E. M., & Perkins, C. E. (2000). An implementation study of the AODV routing protocol. In Wireless Communications and Networking Conference, 2000. WCNC. 2000 IEEE

[5] Shahabi, S., Ghazvini, M., & Bakhtiarian, M. (2016). A Modified algorithm to improve security and performance of AODV protocol against black hole attack. Wireless Networks, 22(5), 1505-1511.

[6] Abdelshafy, M. A., & King, P. J. (2016, January). Resisting black hole attacks on MANETs. In Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual(pp. 1048-1053). IEEE.

[7] Yen, Y. S., Chan, Y. K., Chao, H. C., & Park, J. H. (2008). A genetic algorithm for energy efficient based multicast routing on MANETs. Computer Communications, 31(10), 2632-2641.