IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Comparative Study on Various Security Attacks in MANET

V.Saravanan[*1], Dr. A.Sumathi[2]

[*1]Asst. Prof, IT Department, P.S.V. College of Engineering and Technology, Krishnagiri, Tamilnadu, India

[2]Professor and Head, Department of ECE, Adhiyamaan College of Engg., Hosur, Tamilnadu, India

v_saravanan18@yahoo.co.in

Abstract

As the nodes in the ad hoc network are limited in power backup, computing power and memory, the nodes operate with limited life time and resources to sustain the portability. To maximize the lifetime and healthy of ad hoc networks, the network related transaction must be controlled to avoid the inefficient packet routing (IEPR) attacks. The IEPR will be initiated by a node to make the network to fail by wasting of energy by unwanted packet forwarding process. The IEPR attacks are not specific to the protocol used. This type of attack must be detected and avoided to improve the lifetime of ad hoc networks. In this paper we have discussed about various security issues in MANET and focused more on power usage related attacks.

Keywords: Security, Energy, Unwanted transmitting, Battery Draining, MANET.

Introduction

A mobile ad hoc network consist of mobile nodes without any centralized devices like access points (AP), routers and servers to control the network. Where, the infrastructure network contains all the above said devices to control the nodes. Generally the nodes in the infrastructure have enough resource like power, computing power and memory. So, there will be no problem while designing new protocols or utilities related to infrastructure network since, no need to consider the resource utilization very strictly. But in ad hoc network, the resource like battery power, computing power and memory utilization must be considered strictly while designing new protocols or utilities. As we know that the battery power cannot be increased for a mobile device beyond certain level in order to maintain device portability. Hence battery usage must be limited in mobile devices to have a long battery backup.

In ad-hoc network the mobile nodes will roam without any limitation. So the network topology may change frequently. This makes the path form source to destination to change dynamically and routing process becomes tough in ad hoc networks. Each time the mobiles have to discover the path before routing the packets. The mobile ad hoc network (MANET) routing can be classified into two broad category, they are proactive and reactive. In proactive a table will be maintained by all the nodes, which is similar to infrastructure routing. The table contains the information about the next hope to reach any node in the network with cost. This method of storing the route information may not be suitable for MANET in all the situations. Because, to update the table each and every time when a mobile changes its location may increase the overhead. Reconstruction of table takes more time and periodic exchange of table information with neighbor nodes may decrease the network performance. Two well known algorithms in proactive class are Destination-Sequenced Distance Vector routing (DSDV) and Optimized Link State Routing (OLSR). In [1, 2, 3], many proactive routing algorithms have been discussed in detail.

In reactive routing algorithms, the nodes will find the route dynamically when it needs to send the data to the destination. In this type of routing, delay will be very high comparing with the proactive, since the route discovery process will take time. The reactive routing will discover the route by sending route request packets (RRPs). Increase in RRPs may cause network congestion. The well known algorithms in reactive class are Dynamic Source Routing (DSR) and Ad hoc On-Demand Distance Vector Routing (AODV). Many research have been conducted in past to develop an efficient ad hoc routing in both reactive and proactive classes. Lot of study has been made to compare the performance of reactive and proactive algorithms [4, 5]. The results of these comparative studies are confusing, because both reactive and proactive has their own advantages and disadvantages. So we cannot say which is best,

because it depends on the deployment of the networks.

In addition to reactive and proactive, few more routing algorithms are there namely flow oriented routing, hybrid routing (uses both reactive and proactive), hierarchical routing, power-aware routing, multicast routing, geocasting and host specific routing protocols. These algorithms have their own advantages with few drawbacks. The power-aware routing algorithms are suitable for mobile with very poor battery backup.

As we know that in ad hoc networks Denial of Service Attacks (DoS) are very common today, we need to concentrate more on security issue in ad hoc networking. Especially, on the attacks which try to drain the battery backup and make the node to shutdown. In ad hoc network the battery power is the main resource to keep the network alive. In this paper we focused on power-aware source routing and attacks on ad hoc networks related to battery power.

This paper is organized as follows; in section II we described the basic ad hoc routing algorithms, in section 3 we focused on the power-aware source routing algorithms, in section 4 we have discussed about the attacks in ad hoc networks with a simple method to save the network from battery power related attacks and then we conclude in section 5.

Basic Ad Hoc Routing Algorithms

In this section we discuss in detail about proactive and reactive algorithms with its advantages and disadvantages. The performance of these algorithms has been compared to understand problems rose while routing the packets.

Proactive algorithms

The proactive algorithm updates the routing table frequently. The routing table will be shared between the neighbors via broadcast messages. This broadcast message will be initiated when there is a change in network topology, number of nodes and position of nodes. If the change is very high then, this broadcast message will flood in the network and the network performance will be degraded. Sending of data to the destination can be done faster, comparing the reactive algorithms, since the routing information is ready at any time. The main objective of proactive algorithm is to keep the routing table ready at any time. In section 2.2.1, details of proactive algorithms have given in detail.

Basic work in proactive algorithms

Each node in the MANET will maintain a table T. The table T contains information about all the nodes in network. This table contains maximum of n entries, where n is the number of nodes in a network. Initially the table entry will be empty and it can detect the neighbor nodes and it will start updating the table. The cost (metric) value for same node and the neighbor nodes will be 0 and 1 respectively, since the number of hops need to reach is just one. All the nodes in network will do the same and it will store the cost value for remote nodes (hidden nodes) as infinite (∞). After a regular interval of time, the mobile nodes will start exchange the table with the neighbors. If a node receives the table information from another node then it will check the current table entry with the received one. If the received information contains additional information than the existing table, the new entries must be added to the local table.

Also, if the received cost (metrics) for a remote node is less than the current table entry, it will update the current value by incrementing the received value by one, since the information reached by one hope. After updating the table, at periodic interval the current table status will be broadcast to the neighbors. This process will be repeated in periodic interval and this is how, the mobiles update the table entries for all the nodes in a network. This table entry is useful to route the packets at any time without delay.

Advantages of proactive algorithm

The following are the few advantages of proactive algorithm:

a. The table in each node contains latest information about the network topology at any time.
b. Forwarding or routing packets can be done immediately without finding the path every time.
c. Suitable for the network with rare topological change.

Disadvantages of proactive algorithm

The following are the few drawbacks of proactive algorithm:

a. It performs extremely poor if the no of nodes in the network is high.
b. Unnecessary traffic will be created by table exchange process, hence high energy loss will occur.
c. Nodes life time is limited.

Reactive algorithms

The reactive algorithm provides the connection-oriented service and the main objective is to minimize the packet loss rate. At the time of sending the data, the mobile node will find a path to the destination and then it will send the packet in that right path. This will make the packet to travel shortly, but the time taken for searching the right path will be more. The algorithm is best in some situation, where the mobile node changes its topology frequently. The reactive algorithm will perform poor than proactive

algorithm if the mobile nodes move rarely and the topology is fixed for a long time. The network bandwidth will not be wasted by exchanging routing information as like in proactive. Since the route finding process is initiated at the time of sending the packets, the mobiles will not waste the power for unwanted routing information exchange process.

Basic work in reactive algorithms

The source node will initiate a routing process before sending the data. This can be done by broadcasting of route request. The route request will be received by all the nearby nodes and then it will forward the same to all the nodes in the next hope. The visited node's information will be marked in the route request packet. Also if a node receives same packet from multiple neighbors, it has to drop the packet except the first copy. By doing this the unwanted traffic will be eliminated and the overhead will be reduced. If the destination node receives this route request packet, then it will identify that it is the destination. Now the information stored in the route request packet will be processed to identify the path from source to destination. Similarly the destination can also find the path to the source node to send the reply back. Thus the reactive algorithm will be used to find the path from source to destination and make the communication possible.

Advantages of reactive algorithm

The following are the few advantages of reactive algorithm:

a. Each node may not maintain a table for maintain route information.
b. The routing process is dynamic.
c. Suitable for the network with frequent topological change.
d. No need to waste the bandwidth unless it needs to send the data.
e. Energy will be saved by avoiding unwanted traffic.

Disadvantages of reactive algorithm

The following are the few drawbacks of reactive algorithm:

a. It performs poor than the proactive algorithm when the network topology is fixed for a long time.
b. Battery power will be waste by frequent link failure
c.

Minimized Energy Based Routing

Generally most of the research focused on performance of the network and only few have focused on energy of the network nodes. In [6], Suresh Singh, Mike Woo and C. S. Raghavendra proposed a power aware routing in which the source to destination path is identified before forwarding the packet to minimize the energy loss. The problem is given as follows:

$$Minimize \sum_{i \epsilon path} P(i, i+1)$$

Where P (i, i+1) denotes the power spent by two nearby nodes for sending or receiving data in the route. This is suitable if the transmitting power is fixed for the node and if the transmitting power is dynamic (based on distance). In [7], Lindsey and K. Sivalingam have given the energy for each operation like sending, receiving, broadcast and discard …etc. as follows:

E ($packet$) = $b \times packet\_size + c$

Where b and c denotes the packet size dependent energy consumption and fixed cost that accounts for acquiring channel respectively. The main disadvantage of the above said problem is that the routing algorithm always selects a path which will spend low energy to route the packets. This will make certain mobiles to die very soon and this will make the network to split in to two or more groups. Mobiles in each group can communicate with other mobiles in the same group where the communication is not possible between mobiles in different groups. Thus we need some enhancement in the routing algorithms to make the node to live long. Also we must be aware in ad hoc networks about the attacks related to battery life.

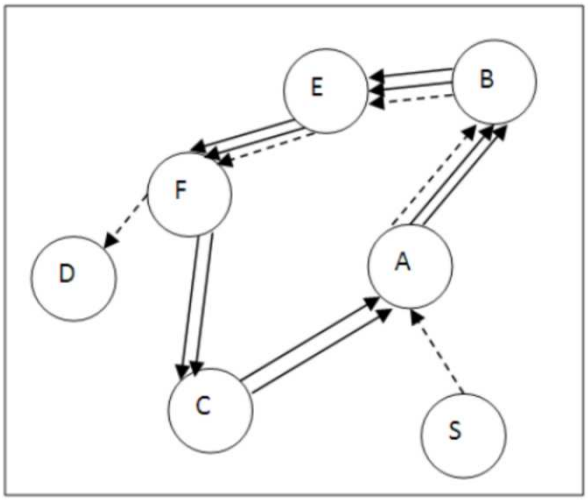

Figure 1: Loopy Path

As we discussed above, the battery power can be wasted by the inefficient routing algorithms and the nodes can die soon which makes the network to get partitioned. This situation should not be encouraged to avoid the path failure and not to make the nodes to spend more time in finding the path.

This situation can be created artificially by the attackers to make the network not available for a long time. This type of attacks related to battery power should be identified and avoided for stable network performance.

Detecting and Avoiding Energy Draining Related Attacks

It is a big challenge to detect and avoid this IEPR attacks, because it is not easy to guess what action will be taken for achieving this attack. Wasting of CPU cycles is one way of attack and wasting of transmission power is another type. In this paper we consider the second case. The impacts of the IEPR attack can be measured by comparing the energy spend by non malicious node with malicious node to send equal size of data with equal distance.

Generally, the nodes in the network will not encourage the cyclic path. That is the loops in the communication path will be avoided. The malicious nodes which send the data will not allow the intermediate nodes to process the header fully. This makes the cyclic path possible by sending packets again and again in the previous paths. In some situation the malicious node makes the packet to travel in the longest path which consumes the network energy more and more. The attacks related to IEPR can be classified in to two categories, the first category is loopy route attacks (LRA) and the second category is path enlargement attacks (PEA).

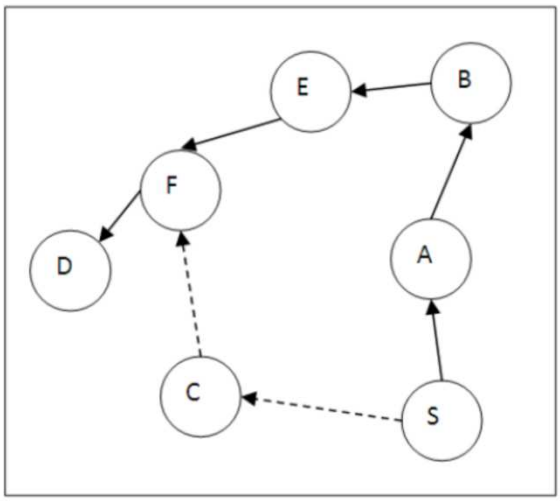

Figure 2: Long Path

In LRA the packets gets forwarded again and again in a limited set of nodes in the network as shown in figure 1. In the PEA the nodes will be selected in such a way that the path should be longer than actual path as shown in figure 2. The working principle of LRA is; the malicious node send packet with path information to reach the destination and the path information will contain sequence of nodes in the order in which it has to send. This sequence may contain repeated nodes. By repeating the node address, the packet will travel in a cyclic path. This makes the node's energy to get wasted multiple times.

The working principle of PEA is the source will send a packet for the destination and if the malicious node receives the packet it will not forward the packet in the actual path. It will try to take worst path by making use of directional antennas. Artificially long path will be selected so that the overall power spend by the network will increase abnormally.

To detect and prevent above said attacks, the network topology has to be discovered. Based on the topological information, every packet has to check whether the packet travels in the topological right path or not. If a node in the network receives packet from its neighbor, it has to check whether the path information contains any repeated node address and if the repetition is detected then the packet will be dropped or the path must be fixed. If the packet contains no repeated node address then the previously visited nodes must be analyzed weather the packet reached here by travelling in the reasonable path. If the previous path contains one or more nodes which is not relevant to the destination, then we will decide that the packet may generated by a malicious node. Then the packet can be dropped to avoid the attack further.

In another case, if the packet is reached to a node in the network that contains no repeated path information and previously visited nodes contain no irrelevant node for a specific destination, then the packet must be forward normally by comparing the number of hops spend by the neighbor nodes for the same destination. If the comparison gives almost equal value then the packet will be forwarded, otherwise it will be dropped. By doing this the node overhead may increase slightly but it will save the network from IEPR attacks.

Conclusion

In this paper a study on various security attacks in MANET have made. We have discussed about various routing algorithms in MANET and we have compared it for performance and security issues. The energy based routing and attacks related to energy of the network nodes have explored. Also, this paper identifies the need for future research on power related attacks in MANET.

References

[1] Perkins, P. Bhagwat "Highly Dynamic Destination-Sequenced Distance Vector

(DSDV) for Mobile Computers" Proc. of the SIGCOMM 1994 Conference on Communications Architectures, Protocols and Applications, Aug 1994, pp 234–244.

[2] Guangyu Pei and Mario Gerla and Xiaoyan Hong AND Ching-Chuan Chiang, "A Wireless Hierarchical Routing Protocol with Group Mobility", IEEE WCNC'99, New Orleans, USA, September 1999.

[3] M. Gerla, J. T. Tsai "Multicluster, Mobile, Multimedia Radio Network" ACM Wireless Networks, VOl 1, No.3, 1995, pp. 255–265.

[4] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), 1998.

[5] C. Mbarushimana and A. Shahrabi. Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks. In Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW), 2007.

[6] Suresh Singh, Mike Woo, C. S. Raghavendra, "Power-Aware Routing in Mobile AdHoc Networks," Proceedings of Mobicom 98 Conference, Dallas, October 1998

[7] S. Lindsey, K. Sivalingam and C.S. Raghavendra, " Power Aware Routing and MAC protocols for Wireless and Mobile Networks", in Wiley Handbook on Wireless Networks and Mobile Computing; Ivan Stojmenivic, Ed., John Wiley & Sons, 2001

[8] P. Appavoo and K. Khedo, SENCAST: A Scalable Protocol for Unicasting and Multicasting in a Large Ad hoc Emergency Network, International Journal of Computer Science and Network Security, Vol.8 No.2, February 2008.

[9] Mesut Günes et al., "ARA – the ant-colony based routing algorithm for manets" Proceedings of the 2002 ICPP Workshop on Ad Hoc Networks (IWAHN 2002), pages 79–85, IEEE Computer Society Press, August 2002

[10] M. Marina, S. Das "On-demand Multipath Distance Vector Routing in Ad Hoc Networks", Proc.2001 IEEE International Conference on Network Protocols (ICNP), pages 14–23, IEEE Computer Society Press, 2001.