A REVIEW: MOBILE AD-HOC NETWORK PROTOCOLS AND SECURITY ISSUES

Ankit Mehto, Hitesh Gupta
Department of Computer Science & Engineering, PIT, Bhopal, India

ABSTRACT

The instant growth of communication takes the attention of researchers in this area. A network has categorized with connecting media. Wireless network is most popular now days due to its infrastructure independence. As the Mobile Ad-hoc network is a classification of wireless network. MANET works with radio waves without need of any central co-ordinating device. It is an autonomous network supporting dynamic topology. Having all these facility MANET also has its own demerits. These issues are related to security and its protocol. This paper gives an idea of mobile Ad-hoc Network, protocol used in MANET and some security issues. This paper also has the discussion about the various attack which are possible in mobile ad-hoc network.

KEYWORDS: MANET, PRNET, Protocols, Attacks.

I. INTRODUCTION

A computer Network is a methodology by which the two or more end users can connect in order to data sharing. To install any network there are three basic needs. These are 1) Computers 2) Connecting Media and 3) Protocol. The network has divided into two categories on the basis of connecting media [1].

Initially the packet radio network was introduced in decade of 70's as a first step of wireless network. It was also known as PRNET. In this network the protocol was the made by ALOHA and Carrier Sense Multiple access (CSMA). This was the first generation of wireless network. In 80's it turned to the second generation. In this time the packet switching has used in order to communicate via wireless network. In 90's the ad-hoc network comes into light. The researchers pay attention to enhance the ad-hoc network [2].

A mobile ad hoc network is a group of nodes that are capable of changing their location dynamically but still they can communicate each other. In this type of network there is no need of centralized device in order to co-ordinate the other nodes. These nodes are able to perform routing also. So Ad-hoc network can install without the predefined infrastructure. This makes Ad-hoc network more flexible. There are many areas where it can apply [1,2].

1) It can use by army. Border is a most sensitive area where communication should take place 24 hours. But some time there is need to establish a communication network instantly. This time Ac-hoc network plays an efficient role.
2) At the time of natural disaster like tsunamis, earth quack, twisters can destroy the infrastructure of whole communication system. So the rescue team can use the Ad-hoc network on the spot.
3) The Mining is a dynamic area which is changed after the mine every day. So the static network may create problem in data communication. This is also a place where Ad-hoc network gives the efficient results.
4) This methodology can also apply for the event management. Due to small area of event with large number of co-coordinating nodes Ad-Hoc network is the best option.

II. MOBILE AD-HOC NETWORK

MANET is a type of wireless network. It is network having mobile node with capability of routing and other features like wired network without any centralized administration. So each node will act as a client and the router. This network uses the dynamic topology concept due to node mobility [3].

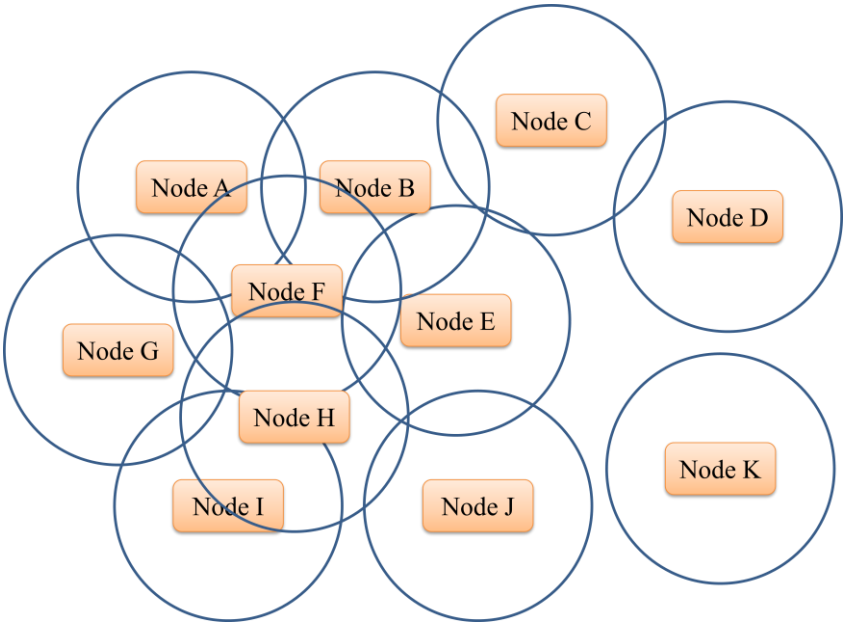

Figure 1: Ad-hoc Network

Figure 1 shows the small Ad-hoc network with their nodes. Here each node has its range. It is must for receiving node to in the network of sender node in order to complete the communication. It is possible that sender and receiver node not connected directly so they can take the help of other adjacent nodes. In above figure node K is an isolated node. This node does not receive any other network so communication never takes place until node K comes under the range of other connected network.

III. ROUTING PROTOCOLS FOR MANET

Protocols is a set of predefine rules, works as an intermediate between two systems. As earlier discussed in communication network protocol is depend on the media used in that network [3, 4, 17]. Routing is crucial task in which the path of destination node will decide. In case of wireless network there are many routing protocols available. These protocol can also use in Mobile Ad-Hoc network. Figure 2 shows the classification of routing protocols of MANET. The table driven protocols share the routing table and perform the routing in the network. The other type of protocol called on demand routing protocol. In these protocol node search will done with the current request of the user [4]. When the route request packet comes the flooding will apply and finally the routing will perform in order to search the path of destination end user. Both the protocols also called the proactive and reactive respectively. The third category is hybrid of the above protocol. This protocol uses both the concepts of proactive and reactive protocols for routing. Apart from this the flow oriented and hierarchical are two other method which can use in order to routing in Ad-hoc Network [5].
In other words the routing protocol is a generalized terminology to define to get the suitable path by which data can efficiently send to the receiver end. Whether, these routing protocols are responsible to perform dynamic routing and information sharing as well [6].

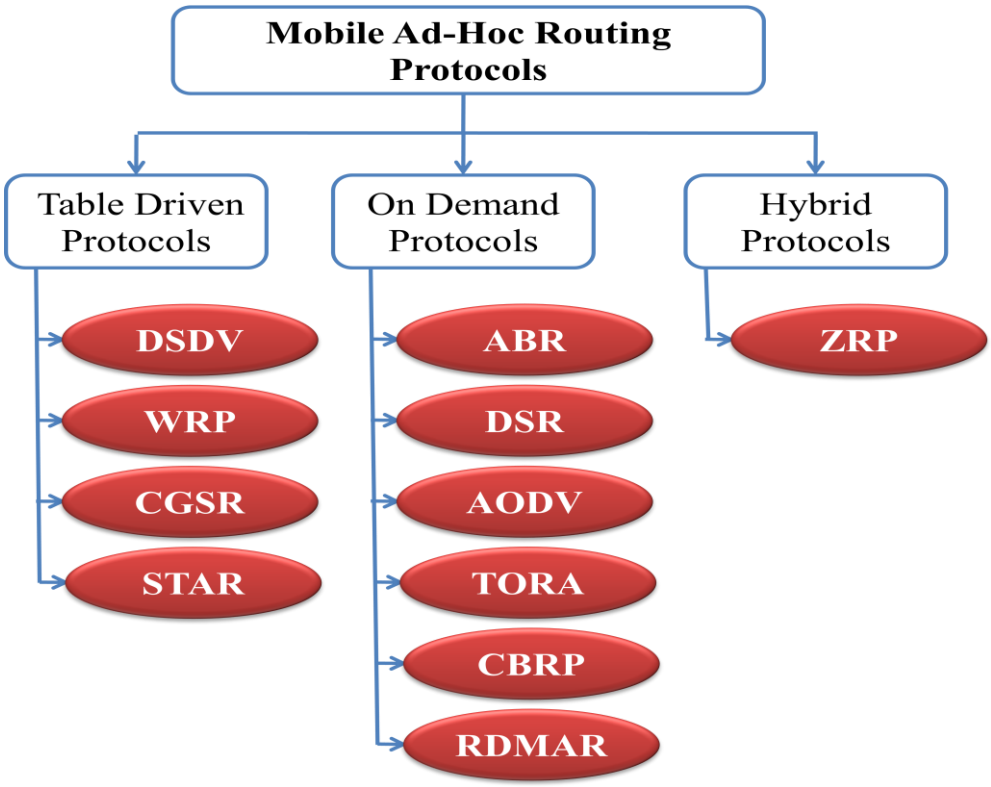

Figure 2 Routing Protocols in Ad-Hoc Networks

IV. ATTACKS IN MANET

Mobile Ad-Hoc network has several loop holes by which the attack in MANET is possible. This attack can do by any node of the network. These nodes itself take part in the malicious actions. This type of nodes called the active node and attack is known as active attack. On other hand some nodes do not involve in the malicious activity directly. This type of action is done by the passive node in passive attack. In both cases such type of node called the malicious node. In Mobile ad-hoc network there are some major concerns in order to secure the network. There all security should be applied in the province of data. These are the principle of network security [7,17].

Authentication: It is based on the right access of a user. In ad-hoc network there may be various anonymous user with the existing users. Which one is authorized to communication? This answer will find out by the authentication policies.

Confidentially: In this concept the message should only know to sender and receiver. None of the nodes have the information regarding the transmitting message.

Integrity: this concept ensures that the message hasn't any changes during the transmission in the network.

Availability: this is necessary for the sender's end. It shows the receiver is online or not.

Non-repudiation: it is concept to prevent the repudiation of message [7,8].

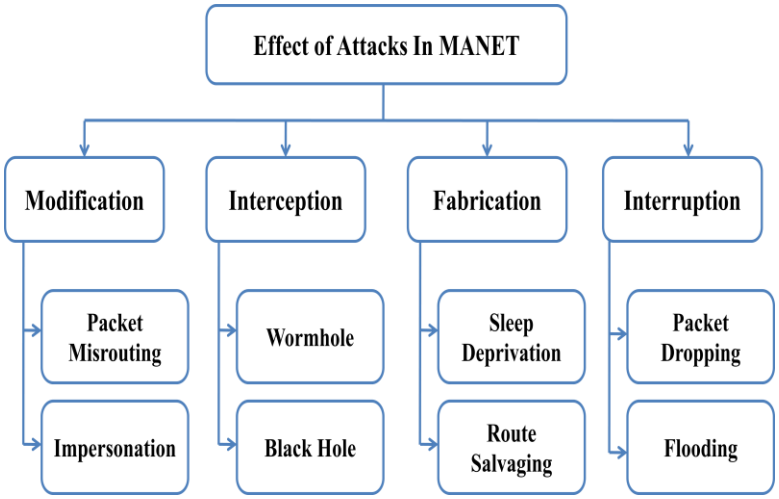

Figure 3 Category of effects by attack in MANET

Ad-hoc Network can install in three basic environments. 1) Open Environment 2) Localized Environment and 3) Organized Environment. Every node of Ad-hoc network exists in one of the above Environment. It seems to be that each Environment has its own security issues. These security issues leave some loop holes to attack in the Ad-hoc Environment. The figure 3 shows the various types of attacks in the ad-hoc network [9,10, 11].

Modification: this type of attack use to customize the routing message. Here one malicious node will change the packet data during the forwarding that message. Here data or message will lose their integrity.

Interception: this type of attack done by the unauthorized user. They show their self as a part of network but they are the malicious node. When they receive the packet of the network they can modify it and forward to next node. The malicious node can able to analyze the data of the packet. In this case the data integrity and confidentiality will lose.

Fabrication: Data modification is not only called the attack. Unused, unwanted packet generation is also comes under the attack. This is known as fabrication attack. Here the malicious node create the large number of packets and send it into the network. When the number of packets goes over the capacity of network then network will fail. Sometime this activity has done by the internal nodes of the network. These nodes are called as misbehaving nodes.

Interruption: In this type of attack the malicious node will prevent the message to receive by the destination node.

V. CONCLUSION

In this study it seems to be that there are many advantages of Ad-Hoc Network. It can apply in Battlefield by Military, Sensor Networks Personal Area Network, Money-making zone, Medical tune etc. in spite of these facility there are some loop holes to establish such kind of network. This paper is a study of various protocols which are used to install the Ad-hoc network. This paper also throws some light on possible attacks in Mobile ad-hoc network. In future there is a possibility to detect & deter melisicious node from attacking in the network.

ACKNOWLEDGEMENT

I would like to say thanks to my guide “Prof. Hitesh Gupta” who gives their knowledge and time in order to complete this paper. This paper will never complete without the support faculty member of CSE department of PCST, Bhopal.

REFERENCES

[1] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks.
[2] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, Wormhole Attacks in Wireless Networks
[3] C. Perkins, E. Belding-Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing," The Internet Society 2003.
[4] Saeed, Nagham H. Abbod, Maysam F.; Al-Raweshidy, Hamed Saffa "MANET routing protocols taxonomy" IEEE 2012, pp 123-128.
[5] P. Gupta and R. Kumar, "The Capacity of Wireless Networks," IEEE Transactions on Information Theory, IT-46(2): pp. 388-404, Mar. 2000.
[6] K. Jain, J. Padhye, V. N. Padmanabhan and L. Qiu, "Impact of interference on multi-hop wireless network performance," Proc. of the MobiCom, Vol. 11, no. 4, pp 471-487, July 2005.
[7] Sheikh, Rashid, Singh Chande, M., Mishra, Durgesh Kumar "Security issues in MANET: A review" IEEE 2010, 1-4.
[8] Hao Yang,Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang, "Security in mobile ad hoc networks: challenges and solutions", IEEE 2004, pp 38-47.
[9] Tara M. Swaminatha and Charles R. Elden, "Wireless Security and Privacy: Best Practices and Design Techniques," Addison-Wesley, 2002.
[10] R. Draves, J. Padhye and B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks," Proc. of MobiCom, pp. 114-128, 2004.
[11] J. So and N. H. Vaidya, "A routing protocol for utilizing multiple channels in multi-hop wireless networks with a single transceiver," Tech. Report, University of Illinois at Urbana-Champaign, Oct. 2004.
[12] A. Qayyum, L. Viennot and A. Laouiti, "Multipoint relaying for flooding broadcast messages in mobile wireless networks", Proc. of HICSS, pp. 3866 – 3875, January 2002.
[13] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum and L. Viennot, "Optimized link state routing protocol for ad hoc networks",Proc. of the IEEE INMIC, pp. 62 – 68, December 2001.
[14] N. Regatte and S. Jagannathan "Optimized Energy-Delay Routing in Ad Hoc Wireless Networks," Proc. of the WWC'05, May 2005.
[15] D. Bertsekas and R. Gallger, Data Networks, New Jersey: Prentice Hall,Inc., 1987, pp. 374-380.
[16] Kannhavong, Bounpadith,Nakayama, Hidehisa; Nemoto, Yoshiaki; Kato, Nei; Jamalipour, Abbas "A survey of routing attacks in mobile ad hoc networks" IEEE 2007, pp 85-91.
[17] Andel T.R. and Yasinsac A., "Surveying Security Analysis Techniques in MANET Routing Protocols," IEEE Communication Surveys & Tutorials, vol.9, 2007, pp. 70-84.

Authors

Ankit Mehto has completed his graduation from Bansal college of Engineering, Mandideep Bhopal

Hitesh Gupta is working in Patel college of science & Technology, Bhopal. He is a Head of Department of Computer science & Engineering Branch.