AN ASSESSMENT OF SECURITY ISSUES AND MANET PROTOCOLS

Dr. Ujwala M. Patil[1] Prashant Udawant[2]

[1]Associate Professor, Department of Computer Engineering,
R. C. Patel Institute of Technology, Shirpur, Dist. Dhule, Maharashtra, India
patilujwala2003@gmail.com
[2]Assistant Professor, Department of Information Technology,
Mukesh Patel School of Technology Management & Engineering, Shirpur Campus
prashant.p.udawant@gmail.com

ABSTRACT

Researchers and technology professionals are now devoting attention to the creation of ad hoc mobile protocols to allow the multiple opportunities presented by mobile devices to increase awareness and popularity of mobile wireless devices. These routing protocols allow mobile devices to increase peer-to-peer information sharing. The Ad-hoc mobile network works in tandem with the radio waves and the information transmission mode is omnibus. There is no Base Station in MANET, and all nodes in the network will serve as central coordinators. MANET supports the dynamic and independent topology of routing. MANET has some security problems. The paper deals with various protocols for dynamic routing and related problems.

KEYWORDS: MANET,DSR , Protocols, Attacks.

INTRODUCTION

Different wireless technologies, such as Bluetooth and other wireless 802.11 standards, help incorporate MANET without a centrally controlled system. The benefits of MANET are reduction in infrastructure costs, avoidance of faulty tolerance, as routing through the forwarding of packets takes place by intermediate node. Because of the lack of centralization, MANET has certain security concerns which affect the reliability of the network.[1,2]

Every node functions as a router in MANET and is transmitted to the packet. With MANET that requires more nodes, more processing power, more memory and more bandwidth are needed.

DCF (Distributed Coordination Function) approaches are used for preventing channel containment because they use CSMA / CA (carrier sense multiple collision avoidance ac Node mobility is also a grave issue, which requires the protection of the existing MANET.

Alternatively Adhoc networks, which do not include internet access as the key requirement is in the context of militarily and catastrophe-related scenarios.

MANET is a network of certain mobile Nodes connected by various dynamic protocols, including AODV, DSR etc. to exchange information.

I) It can be deployed in military areas that need to connect with different mobile devices.

II) It is also used in catastrophic situations involving awareness.
III) It is also used in the mining industry, which involves dynamic routing.[1,2]

MOBILE AD-HOC NETWORK

A Mobile Ad Hoc Network (MANET) is designed for mobile devices connected wirelessly and that are self-configured and have a' infrastructure-free' network. It is a network consisting of a mobile node with protocols and functionality such as the wired network without any centralized administration. Each node acts as a client or as a router using dynamic topology in this type of network [3].

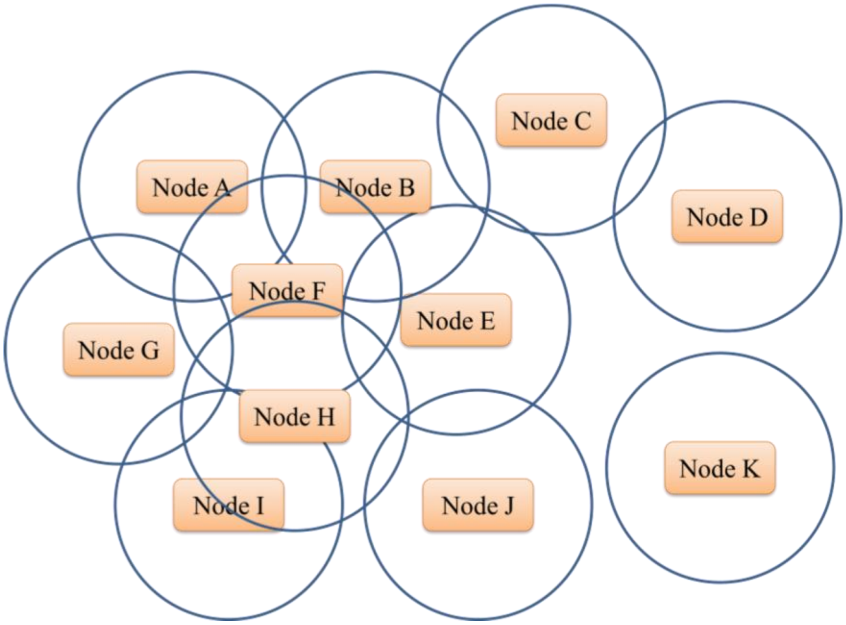


Figure 1: Ad-hoc Network

Figure: 1

An example of a small ad-hoc network is the above diagram. Multiple nodes are connected in the above diagram. Any recipient nodes should be within the sender node continuum which is not within the sender node range, also known as isolated nodes. Many nodes may not be connected directly, they may cooperate with neighboring nodes to communicate. [3,4]

ROUTING PROTOCOLS FOR MANET

Protocols are a set of rules between two structures used as a median. Protocols for network communication depending on the channel type in the network. In order to initiate packet transmission, the direction of the destination node is determined. The MANET protocols are classified as different types of routing. Figure 2.

The first is that table-driven protocols maintain and update the routing tab at each node on a regular basis. This requires Routing Protocols DSVD, WRP, CSGR, STAR. Second, the protocols on demand are performed by the current user's order. These include ABR, DSR, AODV, TORA and CBRP. The last protocol is the Hybrid protocol, which uses the features of the previous protocols. The ZRP protocol is included.

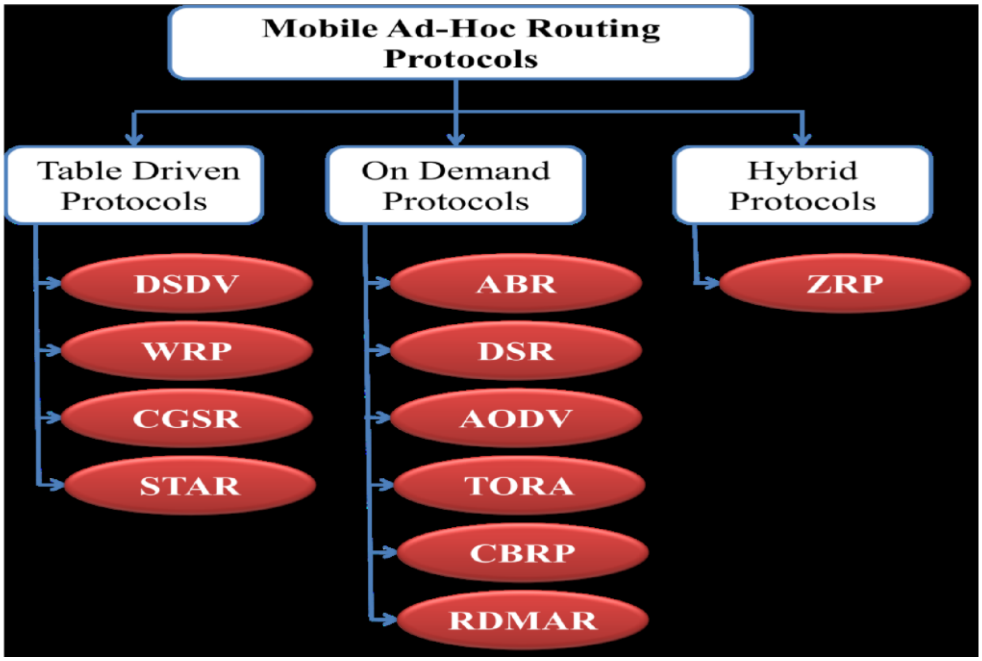


Figure 2 Routing Protocols in Ad-Hoc Networks

ATTACKS IN MANET

The ad-hoc mobile network provides as many openings as possible for attack in MANET. This attack can occur with any node in the network that causes the network to take part in the malicious actions occurring in the network suddenly. The active node is called a type of malicious node and the attack is known as an active assault. However, certain nodes do not engage in malicious activity directly. And this kind of malicious node is known as the passive node and then actively attacks. This type of node is known in both cases as the malicious node. Some major concerns need to be investigated for a secure network on a mobile ad-hoc network (MANET). In certain fields of data law, all protection should be applied. These are the definition of network security for a secure network. [7,8]

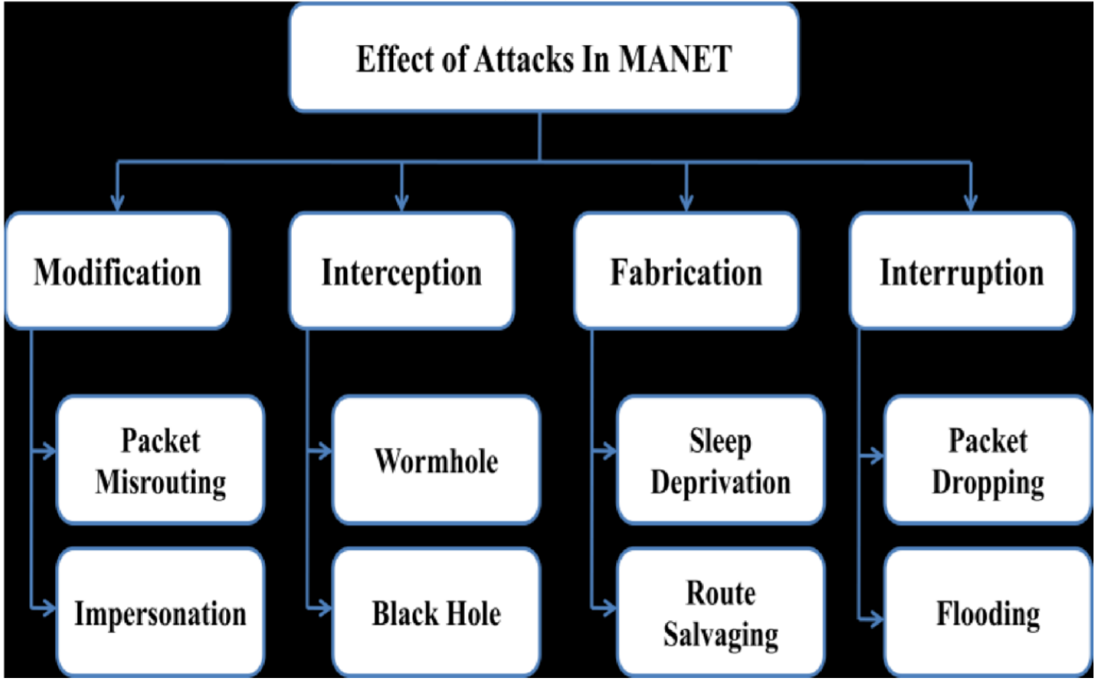
Authentication: It decides whether or not the user is allowed access. There are various anonymous users with different existing users in a mobile ad-hoc network. Which one is allowed to communicate?

Confidentially: The message in the network should only be identified among the sender and the receiver in this definition of confidentiality. None of the nodes in the MANET have knowledge about the message in the network.

Integrity: This makes sure that the message was not changed during network transmission in MANET in this definition of honesty.

Availability: For the end of the sender, it is necessary at MANET. This shows whether or not the receiver is online.

Non-repudiation: The belief that anyone can refute something is to effectively keep the argument from being repudiated.



In these three simple settings, ad-hoc networks can be built.

1) Open Environment

2) Localized Environment

3) Organized Environment.

The above conditions are in each node of the Ad-hoc network. Many safety problems leave a few of the gaps in the above-mentioned setting behind. This figure shows the different kinds of ad-hoc network attacks[9,10, 11].

Manufacturing: Modification of data is under attack and unused unintended packet generation. This is called a manufacturing assault. The malicious node builds a large number of packets and sends them to the network that then passes the network capacity and ultimately fails network. Sometimes the internal nodes of the network conduct this operation. These nodes are referred to as mismatches.

Interception: This type of activity is carried out by an unauthorized person. They cover themselves up as safe nodes, but they're actually malicious. When the data packets of the network are received it can be changed and transmitted to the next node. The malicious node will search the packet data. In such acts as surveillance, data integrity and confidentiality are therefore lost.

Change: It customizes the message for the routing. In this action, during the transmission of that particular message, a malicious node modifies or alters the packet data. Data or messages thus lose their integrity [12]

Interrupt: a malicious node prevents or abandons the message from hitting its target in this type of attack.

CONCLUSION

Upon evaluating both advantages and disadvantages, it seems that the Mobile Ad-hoc Network has numerous benefits. It can be applied in various fields, including military operations, various schools and universities, hospitals and especially smart cities with adequate technology. Notwithstanding all these advantages, there seem to be some shortfalls in the way of success. In addition, the paper contains various protocols used for ad-hoc network deployment. This article highlights possible attacks in the ad-hoc mobile network. Malicious nodes may be identified and deterred from targeting the network for future purposes.

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.