American International Journal of Research in Science, Technology, Engineering & Mathematics

Available online at http://www.iasir.net

ISSN (Print): 2328-3491, ISSN (Online): 2328-3580, ISSN (CD-ROM): 2328-3629

AIJRSTEM is a refereed, indexed, peer-reviewed, multidisciplinary and open access journal published by International Association of Scientific Innovation and Research (IASIR), USA

(An Association Unifying the Sciences, Engineering, and Applied Research)

SURVEY ON MOBILE AD-HOC NETWORK AND ITS APPLICATIONS

Meenakshi Mishra[1], Niketan Mishra[2], Soni Changlani[3]

[1]Student (M.Tech. ECE), [2]Assistant Professor ECE, [3]HOD Dept. of ECE,

Abstract*: This paper is about an introduction or information about mobile ad hoc network (MANET) is generally defined as a network that has many free or autonomous nodes, often composed of mobile devices or other mobile pieces, that can arrange themselves in various ways and operate without strict top-down network administration. There are many different types of setups that could be called MANETs and the potential for this sort of network is still being studied.*

Keywords*: network, MANET, mobile pieces, top-down.*

I. Introduction

Wireless communication between mobile users is becoming more popular than ever before. This is due to recent technological advances in laptop computers and wireless data communication devices, such as wireless modems and wireless LANs. This has lead to lower prices and higher data rates, which are the two main reasons why mobile computing continues to enjoy rapid growth. Wireless Ad hoc networks, have been an interesting area of research for more than a decade now. What makes ad hoc networks interesting and challenging is its potential use in situations where the infrastructure support to run a normal network does not exist. In ad hoc networks all nodes are responsible of running the network services meaning that every node also works as a router to forward the networks packets to their destination. It is very challenging for researchers to provide comprehensive security for ad hoc networks with the desired quality of service from all possible threats. Providing security becomes even more challenging when the participating nodes are mostly less powerful mobile devices. In this paper an effort has been made to evaluate various security designs challenges.

- **Applications**: Because mobile ad hoc networks do not have any fixed infrastructure such as base stations or routers, they are easy and fast to deploy, and have decreased dependence on infrastructures. Mobile ad hoc networks are highly applicable to environment in which no fixed infrastructure is available, either because it may not be economically practically possible to provide the necessary infrastructure or because the expediency of the situation does not permit its installation, such as emergency deployments, disasters, search and rescue missions and military operations. The future commercial use may include but not restrict to conferencing, home networking, and personal area network and embedded computing applications.
- **Low Energy Consumption**: Mobile ad-hoc network is very energy efficient technology the Protocols for MANETs are designed for communication among laptops. Even though laptops are battery-powered, their power budget far exceeds that of a node in a wireless sensor network. Such nodes are often deployed in remote locations. Whether powered by batteries, solar energy, or some other method, reducing energy consumption lessens the weight or extends the lifetime of the package and makes the sensor easier to conceal. Each node in a wireless sensor network only needs to record, transmit, and forward data, unlike a laptop which might have to perform much more complex tasks. As a result, the computational engine in a sensor node consumes significantly less energy than a laptop, and communications must likewise use less energy.
- **Scalability**: Mobile Ad-hoc network has its most important feature of scalability it's an ideal feature for a MANET. This means that as the size of the network increases or the number of nodes increases the wireless network should be able to adapt to the changes and provide consistent performance based on the parameters. This feature is used by researchers to provide scalability to a routing protocol for MANETs. The first method uses hierarchy to provide scalability. The second way to provide scalability is caching. The third way to provide scalability is using geographic information. Using hierarchy to provide scalability is the most widely deployed approach to scale routing as the number of destinations increases.
- **Security issues:** in Mobile Ad-hoc Network security is a very big issue and a bigger challenge too for wireless network in any fixed or wireless network, the security is incorporated at three stages: prevention, detection and cure. Key parts of prevention stage are authentication and authorization. The

authentication is associated with authenticating the participating node, message and any other meta-data like topology state, hop counts etc. Authorization is associated with recognition. Where detection is the ability to notice misbehavior carried out by a node in the network, the ability to take a corrective action after noticing misbehavior by a node is termed as cure. Different possible attacks on ad hoc networks are eavesdropping, compromising node, distorting message, replaying message, failing to forward message, jamming signals etc. The central issues behind many of the possible attacks at any level of security stage are authentication, confidentiality, integrity, non repudiation, trustworthiness and availability.

- There are several proposals available to solve these issues, but are not comprehensive in nature as they target specific threats separately. Therefore there is a strong need to have an efficient security regime which can take care of all the aspects of security.
- **Security threats**: The two broad classes of network attacks are active attacks and passive attacks.
- **Passive Attack**: An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described as
- **Eavesdropping**: The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a network topology between two workstations or tuning into transmissions between a wireless handset and a base station.
- **Traffic analysis**: The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.
- **Active Attack**: An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types masquerading, replay, message modification, and denial-of-service (DoS). These attacks are summarized as:
- **Masquerading**: The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.
- **Replay**: The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.
- **Message modification**: The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
- **Denial-of-service**: The attacker prevents or prohibits the normal use or management of communications facilities.

The consequences of these attacks include, but are not limited to, loss of proprietary information, legal and recovery costs,

II. Conclusion

In this paper, we have discussed about Mobile Ad-hoc Network and its applications, security threats, and some key features of MANET. Mobile Ad Hoc Network (MANET) is a completely wireless connectivity through the nodes constructed by the actions of the network; Wireless communication between mobile users is becoming more popular than ever before. This is due to recent technological advances in laptop computers and wireless data communication devices, such as wireless modems and wireless LANs. This has lead to lower prices and higher data rates, which are the two main reasons why mobile computing continues to enjoy rapid growth.

References

[1] S. R. Das, C. E. Perkins, E. M. Royer, and M. K. Marina, "Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks," IEEE personal Comm,Vol 8,pp.16-28,feb, 2001.

[2] Srdjan krco and marina dupcinov, Improved neighbour detection algorithm for aodv routing protocol, ieee communications letters, December 2003.

[3] Pradeep kumar Mani, David W Petr, Development and Performance Characterization of Enhanced AODV Routing for CBR and TCP Traffic, 864-7762 0-7803-8246-3 2004 IEEE.

[4] Zhao Qiang Zhu Hongbo, "An optimized AODV protocol in mobile ad hoc Network", In Wireless comm. networking & mobile computing 2008(WiCOM'08), 4th international conference on Oct 12-14, 2008, pp.1-4.

[5] Ammar Zahary and Aladdin Ayesh, "On-demand Multiple Route Maintenance in AODV", in Computer Engineering & System, 2008, International Conference on Nov 25-27, 2008, pp.225-230.

[6] Xinsheng Wang, Qing Liu, Nan Xu, The Energy-Saving Routing Protocol Based on AODV, Fourth International Conference on Natural Computation, 978-0-7695-3304-9/08,2008 IEEE.

[7] Mehdi Zarei, Karim Faez, Javad Moosavi Nya, Modified Reverse AODV Routing Algorithm using Route Stability in Mobile Ad Hoc Networks, 978-1-4244-2824-3,2008 IEEE.

[8] YU Bin, SUN Bin, "Modify AODV For MANET/INTERNET Connection Through Multiple Mobile Gateways", ISBN 978-89-5519-139-4 -1519- Feb. 15-18, 2009 ICACT 2009.

[9] Nastooh Taheri Javan, Reza Kiaeifar, Bahram Hakhamaneshi, Mehdi Dehghan"ZD-AOMDV: A New Routing Algorithm for Mobile Ad-Hoc Networks"2009 Eigth IEEE/ACIS International Conference on Computer and Information Science.

[10] Hothefa Sh.Jassim, Salman Yussof, Tiong Sieh Kiong, S. P. Koh1, Roslan Ismail "A Routing Protocol based on Trusted and shortest Path Selection for Mobile Ad hoc Network" Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications 15 -17 December 2009.