ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

MANET: Security Issues

[1] Prashant Johri

[1]Department of Computer Science and Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh

[1] johri.prashant@gmail.com

Abstract: MANET stands for "Mobile Ad Hoc Network." Mobile ad hoc network (MANET) is an independent mobile node device that is linked via wireless connections. Every node not only acts as an end system but also as a packet forwarding router. The nodes are free to move and combine into a network. Such nodes frequently change location. A MANET is a kind of ad hoc network capable of swapping positions and configuring itself on the move. Because MANETS are mobile, special routing algorithms are needed to accommodate the changing topology by using wireless connections to connect to different networks. There is no single protocol that fits perfectly with all the networks. The protocols must be selected on the basis of network features, such as distance, scale and node stability. Work on mobile ad hoc networks is still underway, and work will contribute to even improved protocols, and will likely face new challenges. The paper's main goal is to find out about the security issues and their countermeasures implemented on the Network Layer.

Keywords: MANET, Protocols in Manets, Network security.

INTRODUCTION

Mobile ad hoc networking is one of wireless networking's most creative and demanding fields, one that aims to become ever more prominent in our lives. Ad hoc networks offer a large degree of freedom at a lower cost than other networking systems, comprising of computers that are autonomously self-organizing in networks. A MANET is a group of autonomous mobile users that connect via fairly "weak" wireless links. The network topology will change rapidly and unpredictably over time as the nodes are mobile. The network is decentralized, where all network operation must be conducted by the nodes themselves, including finding the topology and delivering messages. Therefore routing functionality must be incorporated into the mobile nodes. Since the nodes communicate over wireless connections, they have to contend with radio communication effects such as noise, fading, and interference. Furthermore, the connections usually have less capacity than a wired network. Node in an ad hoc wireless network acts as both a host and a router, and network control is spread among the nodes. The topology of the network is usually fluid, as the connection between the nodes will differ with time due to node withdrawals, new node additions and the possibility of having mobile nodes.

Routing Protocols in MANETs:

A routing protocol is used to discover routes between nodes, in order to facilitate connectivity within the network. The primary objective of such an ad-hoc network routing protocol is to create accurate and effective route between a pair of nodes so that messages transmits in a timely fashion. The design of the road should be achieved with a reduced usage overhead and bandwidth. An Ad-hoc routing protocol is a convention or standard that controls how nodes agree on how to route packets in a MANET between computer devices. Nodes in ad-hoc networks do not have a priori knowledge of network topology around them, they have to discover it. The basic idea is that a new node must signal its arrival and respond to notifications transmitted from its neighbors.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

Network Security in MANETs:

Specific factors influence the security issues and architecture accordingly are Environment, origin, range, service quality, and safety criticality in particular, are variables that affect network security. The way encryption is applied differs as network size changes. If the nodes are very distant from each other, there is an increased risk of security attack. On the other side, if the nodes are so similar to each other that they will potentially have a physical contact, any secret information (e.g. hidden keys) between the nodes is communicated by putting them at air. That would increase the security level, since physical communication lines are better than wireless communication lines. The last element defined in terms of security for Ad Hoc networks is safety criticality. It suggests that before we talk about the ways to implement protection, we need to carefully consider if security is required at all or whether it depends if someone else sees what packets are being sent and what they hold. Is the network compromised if there is addition of new packets and retransmission of old ones? Security issues aren't always important, but it could cost a great deal to maintain. There is sometimes trade-off between safety and cost.

Problems with ad-hoc routing protocols:
Causes
Nodes exchange information about the network topology through ad-hoc routing protocols, because the nodes are also routers. It reality is also a significant weakness because a compromised node may give bad information for redirecting or simply stopping traffic. In addition, in terms of security, we may claim routing protocols are very weak. This section is intended to give an overview of the triggers of adhoc routing protocol problems.

A) Ad-hoc network architecture: Ad-hoc networks do not have a set fixed framework and therefore nodes themselves have to contend with packet routing. Each node is dependent on the other adjacent nodes to relay packets.

B) Complex topology of ad-hoc networks: node structure may change due to the versatility feature of ad-hoc networks: they include nodes that may alter their positions regularly. Because of this, we're concerned about the complex topology of these networks, which is a key feature that causes problems: as several adhoc networks merge together, duplications of IP addresses will arise, and it's not that simple to solve.

C) Wireless communication problems: wireless networks have low noise and signal distortion safety, and routing based control messages and is adversely affected. A malicious intruder just spy the information circulating within this network on the line, jam, interrupt or distort it.

D) Implicit neighborhood confidence relationship: Real ad hoc routing protocols presume all participants are trustworthy. Instead, this helps malicious nodes to act directly and threatens to paralyze the entire network, merely by providing false information.

Types of Attacks in Manet:

Ad-hoc networks are more easily attacked than wired networks, owing to their unique nature. Two types of attacks are distinguishable: passive attacks and aggressive attacks. A passive assault does not interact with the protocol's service, but by listening to traffic attempts to find valuable information. Alternatively, an aggressive attack injects random packets and attempts to interrupt network service to restrict capacity, obtain authorization, or draw packets for other nodes. The MANET routing protocols are quite vulnerable since attackers will quickly get details about topology of the network.

Attacks Use Modification:

One of the simplest ways for a malicious node to interrupt the good functioning of an ad-hoc network is to declare better routes than the other nodes (to access certain nodes or just a single some). This type of attack is based on changing the metric value for a path, or

changing the fields of control post.
Assaults use impersonation: such assaults are termed spoofing as the malicious node covers the actual IP or MAC addresses and uses another. Because existing ad-hoc routing protocols such as AODV and DSR do not authenticate the IP address of the source, a malicious node uses spoofing to initiate several attacks. For example, a hacker might create network loops to isolate a node from the rest of the network. To do this, the intruder merely needs to take other node's IP address in the network and then use it to announce new path (with the smallest metric) to the other nodes. By doing so, he will easily change the topology of the network, as he wishes.

Security Threats in Network Layer:

Within MANET, the nodes often act as routers that discover and manage routes to other nodes in the network. Establishing an effective and secure path between the interacting parties is the primary concern of the routing protocols of MANET. Some routing process attack will interrupt total connectivity and paralyses the entire network. Therefore, network layer security plays an important role in network security as a whole.

Network Layer Attacks:

Through security research a number of attacks through network layer were found and analyzed. An intruder will capture network traffic, insert itself into the route between source and destination and thus control the flow of network traffic. Attacks at various stages shall be as follows:
1. Attacks at the routing discovery phase
2. Attacks at the routing maintenance phase.
3. Attacks at data forwarding phase.
4. Attacks on particular routing protocols.
Attacks by Names are as:
1. Wormhole attack.
2. Black hole attack.
3. Byzantine attack.
4. Rushing attack.
5. Resource consumption attack.
6. Location disclosure attack.

Security mechanisms:

In counter malicious attacks a number of security mechanisms were developed. The first line of security is provided by traditional methods such as authorization, access control, encryption and digital signature. As a second line of defence, detection systems for intrusion and compliance frameworks for cooperation introduced in MANET also defend against attacks or impose cooperation, minimizing selfish node actions.
Preventive mechanism: The modern methods for authentication and encryption are based on cryptography, including asymmetric and symmetric cryptography. Cryptographic primitives such as hash functions (message digests) is used to boost the security of data in transmission. Threshold cryptography can be used to conceal data by splitting it into several shares and also use a digital signatures to obtain data integrity and authentication services. Consideration must also be provided to the physical safety of mobile devices, since the hosts are usually small devices that are physically vulnerable.

Reactive mechanism:

A second line of defence is an intrusion detection device. Misuse and irregularities are commonly used for identification. A method of abuse detection aims to identify improper behavior based on patterns of well-known attacks, but lacks the ability to recognize any attacks which were not noticed during pattern creation; anomaly detection tries to systematically classify usual or expected behaviour. This collects data over a period of time from normal user behavior and then use predictive tests to determine anomalous behavior with a high level of confidence. Throughout reality all methods might be combined to make attacks more successful.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

Countermeasures on Network Layer Attacks:

Throughout MANET, network layer is more vulnerable to attacks than any other framework. In this framework a number of health risks are placed. The first line of defence is the use of reliable routing protocols. The aggressive attack like routing code alteration may be avoided by authenticating the origins and validity function of the packet. Of eg, for this reason the digital signature, message authentication code (MAC), hashed MAC (HMAC), single-way HMAC key chain is used to track wormhole attacks by an unchangeable and distinct physical measure such as time delay or geographical location.

LITERATURE REVIEW

In this essay we address the state of the art of ad hoc networking for (mobile) multihops. This model has often been associated with the approaches produced within the IETF MANET working group, and it is named the MANET paradigm for that purpose. They don't match though, so they obviously diverged in the last decade. In this paper, we continue from the explanations why the MANET model did not have a major impact on machine communications, and address the development of the multihop ad hoc networking paradigm by drawing on the lessons learned from MANET research[1]. In this paper e present aspects related to this field to help researchers and developers understand and distinguish in one solid document the main features surrounding VANET, highlighting the need to go through other relevant papers and articles starting with VANET architecture and ending up with the most appropriate simulation tools to simulate VANET protocols and applications[2]. This paper describes the fundamental problems of ad hoc network by providing context to its related research including MANET's definition, functionality, status, and vulnerabilities. This paper provides a review of the routing protocols and their analysis. Also include the various challenging issues, emerging applications and MANET's future trends [3]. This paper describes ad hoc network's fundamental problems by providing context to its related research including the concept, features, status, and weakness of MANET's. This paper includes a study of, and examination of, the routing protocols. Include also the numerous difficult problems, new technologies and future trends in MANET[4]. The experimental results recorded indicate the efficacy and usefulness of the proposed solution (e.g., minimal overhead coordination). Ubiquitous smart environments, equipped with low-cost and easy-to-deploy wireless sensor networks (WSNs) and widespread ad hoc mobile networks (MANETs), open up brand new opportunities for wide-ranging urban monitoring. Nonetheless, MANET and WSN integration paves the way for the creation of brand new networking networks on the Internet of Things (IoT), with a high potential for a wide range of applications across different domains[5]. This paper discusses the state of the art of ad hoc (mobile) multi-hop networking with a view to presenting the current status of research activities and identifying consolidated research areas with limited research opportunities and hot and emerging research areas that require further research. We begin by briefly addressing the MANET model, and why MANET protocol analysis is now a cold research topic[6]. The purpose of this study is to figure out which protocol is more vulnerable to attack from the wormhole. The findings of the OPNET simulation indicate the latency, end-to-end delay, network load and traffic obtained on AODV and OLSR in MANET, with Wormhole and without Wormhole. The results indicate that AODV is more vulnerable to wormhole attacks than OLSR is. MANET's implementation using constructive routing protocol is therefore more trustworthy relative to the reactive one[7]. Proposed a total solution that involves network interfaces, spectrum allocation, node implementation, MANET routing and usability patterns and finally IoT devices that are tested using Omnet++ simulators and demonstrated their efficiency and viability. In this paper we investigate the range of available MANET routing protocols and discuss the functionalities of several ranging from early protocols such as DSDV to more advanced ones such as MAODV, our study of protocols focuses on Perkins ' work in developing and improving MANET routing. A selection of literature

on the field of MANET routing has been established and examined, as well as literature on the subject of AODV-based MANET protocols as this may be the most common MANET protocol[8]. This article examines the range of available MANET routing protocols and addresses functionalities varying from early protocols such as DSDV to more advanced ones such as MAODV, our protocol review reflects on the research of Perkins in designing and strengthening MANET routing. A collection of literature on the field of MANET routing and literature on the topic of AODV-based MANET protocols have been developed and reviewed, as this may be the most popular MANET protocol[9].

CONCLUSION

Ad-hoc networks are thus proving to be susceptible to different types of attacks since they are less network complex, wireless and connectivity. In addition to all these risks, there are also routing protocols to allow them more safe and error-free networks there by admiring the ultimate goal of ad hoc networks, which is to achieve instant networks irrespective of the types of nodes or environments that prevail in this article. Remote ad hoc networks have the ability to set up on-fly networks in a harsh environment where a conventional network infrastructure may not be installed. In our study, we have classified a variety of different layer-related attacks and found that network layer is most vulnerable than all other layers in MANET. The separation of threats on the basis of different layers makes the protection breaches in ad hoc networks readily understood. A response to' How security services like anonymity, privacy, and authentication be accomplished across ad hoc mobile networks? Which move to take? On the basis of a particular attack, security services is achieved by following preventive and reactive countermeasures. We've also mentioned' what are the countermeasures in Network Layer for each type of attack? And concentrate on the potential countermeasures actually being used and specifically designed for MANET.

REFERENCES

[1] M. Conti and S. Giordano, “Mobile ad hoc networking: Milestones, challenges, and new research directions,” *IEEE Commun. Mag.*, 2014, doi: 10.1109/MCOM.2014.6710069.

[2] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, “A comprehensive survey on vehicular Ad Hoc network,” *Journal of Network and Computer Applications*. 2014, doi: 10.1016/j.jnca.2013.02.036.

[3] P. Goyal, V. Parmar, and R. Rishi, “MANET: Vulnerabilities, Challenges, Attacks, Application,” *IJCEM Int. J. Comput. Eng. Manag. ISSN*, 2011.

[4] A. Dorri and S. R. Kamel, “Security Challenges in Mobile Ad Hoc Networks: A Survey,” *Int. J. Comput. Sci. Eng. Surv.*, 2015, doi: 10.5121/ijcses.2015.6102.

[5] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, “Convergence of MANET and WSN in IoT urban scenarios,” *IEEE Sens. J.*, 2013, doi: 10.1109/JSEN.2013.2272099.

[6] M. Conti *et al.*, “From MANET to people-centric networking: Milestones and open research challenges,” *Comput. Commun.*, 2015, doi: 10.1016/j.comcom.2015.09.007.

[7] M. Sadeghi and S. Yahya, “Analysis of Wormhole attack on MANETs using different MANET routing protocols,” 2012, doi: 10.1109/ICUFN.2012.6261716.

[8] A. Hinds, M. Ngulube, S. Zhu, and H. Al-Aqrabi, "A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)," *Int. J. Inf. Educ. Technol.*, 2013, doi: 10.7763/ijiet.2013.v3.223.

[9] J. Whitbeck and V. Conan, "HYMAD: Hybrid DTN-MANET routing for dense and highly dynamic wireless networks," *Comput. Commun.*, 2010, doi: 10.1016/j.comcom.2010.03.005.