Impact
Factor
2. 147

ISSN 2349-638x

Reviewed International Journal

AAYUSHI INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (AIIRJ)

Monthly Publish Journal

VOL-III ISSUE-VI June 2016

Address
•Vikram Nagar, Boudhi Chouk, Latur.
•Tq. Latur, Dis. Latur 413512
•(+91) 9922455749, (+91) 9158387437

Email
•aiirjpramod@gmail.com

Website
•www.aiirjournal.com

CHIEF EDITOR – PRAMOD PRAKASHRAO TANDALE

The Safety Disputes and Necessities in MANETs: A Analysis

Patange V. N.
Research Scholar, Department of Computer Science,
JJT University,
Chudela Dist.Jhunjhunu, Rajasthan
vishal.ptnge@rediffmail.com

Abstract:

The security problems with wireless technology without centralized control, along with their existing fixes and needs, were discussed in this study. Due to its inherent vulnerability, the MANET is subject to several security risks that disrupt packet exchange. First, we discussed the security requirements for mobile ad hoc networks and explained the primary vulnerability in the MANET. Finally, the security solutions that are currently available for mobile ad hoc networks are detailed here.

Keywords: Attacks, MANETS, Security.

1. Introduction

The proliferation of wireless technology and its new innovations has led to an increase in mobile computing devices. In the computer science community, the gadgets—such as laptops, PDAs, and digital devices—become research areas (Macro Conti, 2003). Every useful piece of information is available to the user at any time and from any location, and wireless networks are used to connect them. Self-networks and a transient network topology architecture are features of this mobile ad hoc network. Without any existing communication infrastructure facilities, the gadgets or individuals are able to communicate with one another. Corson, M. S. (1999). Node scans in mobile ad hoc networks connect directly with every other node within their radio ranges, whereas nodes outside of this range communicate with one another through an intermediary node or nodes. In these two scenarios, every node involved in the communication has taken part. The following are typical characteristics of the mobile ad hoc network:

Ketan and Amitabh Mishra (2003).

1 Wireless connectivity between nodes are unreliable. The wireless connections between mobile nodes in the ad hoc network are inconsistent for the communication participants due to the wireless nodes' limited energy supply and mobility.

2 The topology is always shifting. The mobile ad hoc network's topology is always changing due to the nodes' constant movement. The nodes can constantly enter and exit the radio range of other nodes in the network, and the routing information is always changing as a result of the nodes' movement.

3. The absence of security features in wireless routing protocols that are statically established and not intended for ad hoc settings. Ad hoc networks' dynamic topology necessitates that every pair of neighbouring nodes be included in the routing problem in order to guard against potential attacks that attempt to exploit flaws in the statically set routing protocol.

The remainder of the document is structured as follows: The primary weaknesses that render mobile ad hoc networks insecure are covered in Section 2. We examine the viability of the existing security solutions for mobile ad hoc networks in Section 3. The paper's conclusion and a list of possible next projects are presented in Section 4.

2. Vulnerabilities of The Network

Compared to typical wired networks, mobile ad hoc networks are significantly more vulnerable, and maintaining security in these networks is far more challenging. The several vulnerabilities present in mobile ad hoc networks are covered in this section.

2.1. Lack of Secure Boundaries The significance of this weakness is obvious: unlike the traditional wired network, which has a defined line of defence, the mobile ad hoc network lacks a distinct secure boundary. The freedom to join, exit, and move within the network is the root cause of this vulnerability in mobile ad hoc networks. Before committing malicious acts against targets in a wired network, adversaries must physically get access to the network medium or even go past multiple tiers of defence, including firewalls and gateways.

2.2. Threats from Compromised nodes Inside the Network : We primarily addressed the vulnerability of the mobile ad hoc network's lack of distinct secure borders in the preceding part, which could lead to a variety of link assaults. These link assaults focus on the connections between the nodes and attempt to destroy them by engaging in certain malevolent actions. Other attacks, on the other hand, seek to take control of the nodes themselves by unethical ways, then utilize the compromised nodes to carry out additional malevolent deeds. This vulnerability can be thought of as the dangers posed by the network's compromised nodes.

2.3. Lack of Centralized Management Facility : Because ad hoc networks lack a centralized administration tool, like a name server, they are susceptible to certain issues. Let's talk about this issue in further detail now. First of all, the lack of centralized management tools makes it extremely challenging to identify assaults since it is challenging to keep an eye on traffic in a large-scale, highly dynamic ad hoc network.

2.4. Restricted Power Supply : As everyone is aware, because ad hoc network nodes are mobile, it is typical for them to rely on batteries as a power source. The nodes in the mobile ad hoc network must take into account the limited battery power, which will result in multiple issues, whereas the nodes in the wired network do not have to worry about the power supply issue because they can obtain an electric power supply from outlets, which typically means that their power supply should be roughly infinite.

2.5. Scalability : Lastly, when discussing the weaknesses in the mobile ad hoc network, we must consider the issue of scalability. Because of the mobility of the nodes in the mobile ad hoc network, it is difficult to predict how many nodes the network will have in the future. This is in contrast to the traditional wired network, which has a scale that is typically predefined when it is designed and will not change much during use.

Therefore, the protocols and services used in the ad hoc network, including the routing protocol and the key management service, should be able to adapt to the network's constantly shifting scale, which might vary from decades of nodes to hundreds or even thousands of nodes.

3. Security Solutions of Manets

The previous section discussed a number of flaws that could make mobile ad hoc networks insecure. However, understanding the existing weaknesses of the mobile ad hoc network is far from our ultimate goal of protecting it. As a result, we need to find strategies for protecting the mobile ad hoc network. In this section, we look at some security measures to protect the mobile ad hoc network from malicious activity.

3.1. Security Criteria : Identifying how to determine whether a mobile ad hoc network is secure or not, or what should be included in the security criteria for the mobile ad hoc network when we wish to inspect the security state of the mobile ad hoc network, is something we believe is necessary before surveying the solutions that can help secure the mobile ad hoc network. Here, we provide a quick overview of the commonly used standards for determining the security of mobile ad hoc networks.

3.1.1. Availability : Regardless of its security state, a node should be able to continue providing all of the services that have been designed [4]. During denial-of-service attacks, which can target any node in the network, certain self-centred nodes disable some network services, such the routing protocol or the key management service, making this security criterion vulnerable.

3.1.2 Integrity:-Integrity guarantees the identity of the messages when they are transmitted. Integrity can be

3.1.3Resource availability:-MANETs are composed of low power device with restricted energy, restricted power supply, bandwidth and CPU, as well as low memory.

3.1.4. Scalability:- due to mobility of nodes, scale of ad hoc network always affected. So scalability is a major issue in MANET security.

3.1.5. Cooperativeness:- routing algorithm for MANETs typically assumes that nodes are cooperative and non-malicious.as a result a spiteful attacker can become an important routing agent and disrupt network operation by disobeying the protocol specifications.

3.1.6. Lack of centralized management:- the lack of management makes to difficult for detection of attacks because it is not easy to observe the traffic in a highly dynamic and large scale ad-hoc network .lack of centralized management will obstruct trust management for nodes.

3.1.7. Dynamic topology- nodes move within the network. This mobility involves the network topology confirms the connectivity between hosts that change quickly and accidently. Hence, the control and the management of MANET surroundings will have to be distributed among the participating nodes of the network.

3.2 wireless network attack in MANETS

Wireless ad hoc network security is a major concern.The first step in developing a strong security solution is always to understand attackers. MANET is more vulnerable to assaults than wired networks because it lacks a shared wireless intermediate and any central coordination tools. MANET is vulnerable to several types of attacks. For secure transmission in sequence, communication security in MANET is important. These assaults fall into

3.2.1 Passive Attacks : Attacks that do not interfere with a network's ability to function normally are known as passive attacks. Attackers intercept network traffic without changing it. If an attacker can also decipher data obtained by spying, the secrecy requirement may be broken. Since the network's ability to function is unaffected, detecting these attacks is challenging.

3.2.2Active Attacks : Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. Active attacks can be internal or external.

External attacks – External attacks are accepted out by nodes and cannot fit in the network. It causes unusual nodes these nodes sends false routing information or causes unavailable of services

Internal attacks- Internal attacks are from comprised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized contact and impersonates as a valid node. It can analyze trade between other nodes and may participate in other network activities.

ACTIVE ATTACKS

Black Hole Attack : In this attack, all nearby nodes direct packets towards the attacker by advertising a zero metric for all destinations. By sending fictitious routing information and claiming to have the best path, a malicious node tricked other good nodes into sending data packets via it. Instead than forwarding all packets that it receives, a rogue node drops them all. An attacker uses a flooding-based protocol to listen to the queries.

Sinkhole : In a sinkhole attack, a compromised node tries to attack the data to it from all neighboring nodes. So, practically, the node eavesdrops on all the data that is being communicated between its neighboring nodes. Sinkhole attacks can also be implemented on ad hoc network networks such as AODV by using flaws such as maximizing the sequence number or minimizing the hop count, so that the path presented through the malicious node appears to be the best available route for the nodes to communicate.

Spoofing Attack : By pretending to be another node in the network, the attacker in a spoofing attack gets communications intended for that node. This kind of assault is typically carried out to obtain access to the network in order to launch other attacks that have the potential to severely damage the network. Any hostile node with sufficient network knowledge can launch this kind of assault by creating a fake ID of one of its member nodes. Then, using that ID and a financial incentive, the node can trick other nodes into setting up a path towards it instead of the actual node.

RERR Generation : Malicious nodes can prevent communication between any two nodes by sending RERR message to some node along the path. The RERR message when flooded into the network may cause the breakdown of multiple paths between various nodes of the network, hence causing a no. of link failures.

Jamming : In jamming, attacker initially keep mounting wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.

Rushing Attack : Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path exists between the two ends of the wormhole, the tunneled packets can propagates faster than those through a normal multi hop route. The rushing attack can act as an effective denial of service attack against all currently proposed on demand MANET routing protocols, including protocol that were designed to be secure , such as ARAN and Ariadne

Byzantine attacks : A compromised with set of intermediate nodes that working alone within network carry out attacks such as creating routing loops forwarding packets through non-optimal paths or selectively dropping packets which results in disruption or degradation of routing service within the network.

Replay Attack : An attacker that performs a replay attacks are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of route, but can also be used to determine poorly designed security solutions.

Flooding : Malicious nodes may also inject false packets into the network, or create ghost packets which loop around due to false routing information, effectively sing up the bandwidth and processing resources along the way.

PASSIVE ATTACKS

Traffic Analysis

Traffic analysis is a passive attacks used to gain information on which nodes communicates with each other and how much data is processed.

Eavesdropping

The word "eavesdrops" refers to overhearing without making any further effort. This involves the unintended recipient intercepting, reading, and conversing with the communication. A wireless medium is shared by mobile hosts in mobile ad hoc networks. The vast majority of wireless communications broadcast by nature and require RF spectrum. Fake messages can be introduced into a network and transmitted messages can be intercepted.

Traffic Monitoring

It can be developed to identify the communication parties and functionality which could provide information to launch further attacks. It is not specific to MANET. Other wireless network such as cellular, satellite and WLAN also suffer from these potential vulnerabilities.

Syn flooding

This attack is denial of service attack. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resources constraints for legitimate nodes.

Snooping

Snooping is unauthorized access to another person's data. It is similar to eavesdropping but is not necessarily limited to gaining access to data access to data during its transmission. Snooping can include casual observance of an email that appears on another computer screen or watching what someone else is typing. .

4.Security Schemes in the MANETS

Intrusion Detection Techniques

Intrusion detection is not a new concept in the network research. According to the definition in the Wikipedia, an Intrusion Detection System (or IDS) generally detects unwanted manipulations to systems. Although there are some differences between the traditional wired network and the mobile ad hoc network, intrusion detection technique, which is developed first in the wired network and has become a very important security solution for the wired network, has also gained some attentions from the researchers when they explore the security solution for the mobile ad hoc network. In the following, we discuss some typical

The Intrusion detection techniques in the mobile ad hoc networks has explained in details,

Intrusion Detection Techniques in MANET

The first discussion about the intrusion detection techniques in the mobile ad hoc networks was presented in the paper written by Zhang et al.

In this paper, a general intrusion detection framework in MANET was proposed, which was distributed and cooperative to meet with the needs of MANET. The proposed architecture of the intrusion detection system is shown below in Figure 1

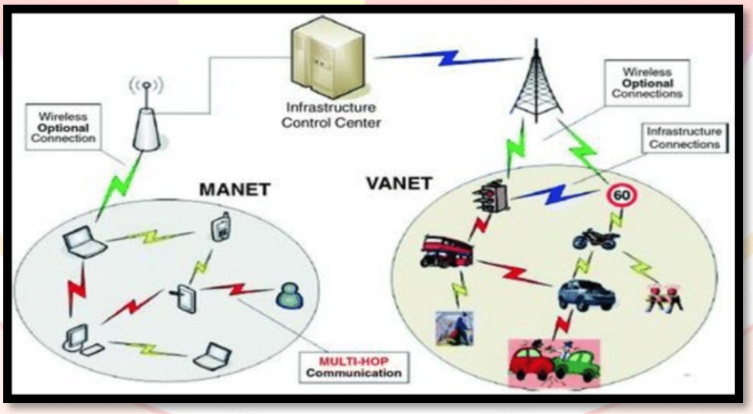
Infrastructure Control Center
Wireless Optional Connection
Wireless Optional Connections
Infrastructure Connections
MANET
VANET
60
MULTI-HOP Communication

Figure 1: architecture of MANETS

Cluster-based Intrusion Detection Technique for Ad Hoc Networks

We have discussed cooperative intrusion detection architecture for the ad hoc networks in the previous part, which was first presented by Zhang et al. However, all of the nodes in this framework are supposed to participate in the cooperative intrusion detection activities when there is such a necessity, which cause huge power consumption for all the participating nodes. Due to the limited power supply in the ad hoc network, this framework may cause some nodes behave in a selfish way and not cooperative with other nodes so as to save their battery power, which will actually violate the original intention of this cooperative intrusion detection architecture. To solve this problem, Huang et al. present a cluster-based intrusion detection technique for ad hoc networks M. Corner and B. Noble(2002).

Misbehavior Detection through Cross-layer Analysis

Multi-layer intrusion detection technique is another potential research area that Zhang et al. point out in their paper [18]. However, they seem not to explore deeper in this area. In this part, we will discuss the cross-layer analysis method presented by Parker et al. (2002).

Intrusion Detection Techniques in MANET:

In this part, we survey several typical intrusion detection techniques in the mobile ad hoc networks. Due to the constantly changing topology and limited battery power, the intrusion detection mechanism in the mobile ad hoc networks should be cooperative and energy-efficient, which are shown in the two papers written by Zhang et al. and Huang et al. respectively Due to the mobility of the nodes and the continuously changing topology in the ad hoc network, it is sometimes relatively hard to collect the enough evidences for a node if it only relies on the single-layer detection method, where it may be vulnerable for the setting of the threshold. As a result, the concept of multi-layer or cross-layer detection mechanism is raised;

5. Secure Routing Techniques in Mobile Ad Hoc Network

Finally we move to a secure ad hoc routing approach using localized self-healing communities.

Defense Method against Wormhole Attacks in Mobile Ad Hoc Networks

Wormhole attack is a threatening attack again routing protocols for the mobile ad hoc networks. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and replays them there into the network. The replay of the information will make great confusion to the routing issue in mobile ad hoc network because the nodes that get the replayed packets cannot distinguish it from the genuine routing packets. Moreover, for tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make

The tunneled packet arrives with better metric than a normal multi-hop route, which makes the victim node be more likely to accept the tunneled packets instead of the genuine routing packets. As a result, the routing functionality in the mobile ad hoc network will be severely interfered by the wormhole attack.

Defense Mechanism against Rushing Attacks in Mobile Ad Hoc Networks

Rushing attack is a new attack that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols. principles of which are discussed below H. Goto, et.al. (2007).Watchdog determines misbehavior by copying packets to be forwarded into a buffer and monitoring the behavior of the adjacent node to these packets. Watchdog promiscuously snoops to decide if the adjacent node forwards the packets without modifications or not.

Watchdog and Path rater

Watchdog and Path rater are two main components of a system that tries to improve performance of ad hoc networks in the presence of disruptive nodes, the specific working

A Secure Ad Hoc Routing Approach using Localized Self healing Communities

The paper first describes two routing attacks that use non-cooperative network members and disguised packet losses to deplete ad hoc network resources and to reduce ad hoc routing performance, which are called RREQ resource depletion and RREP packet and data packet loss, respectively H. Goto, Y. et al. (2007). These two attacks have not been fully addressed in previous research, so it is necessary to introduce these two attacks first.

Secure Routing Techniques in Mobile Ad Hoc Networks:

In this part, we mainly discuss various secure routing techniques that can help ensure the ad hoc routing security. Some of them deal with specific attacks that aim to disturb the ad hoc routing services, and provide some solutions to help defend against these attacks; whereas other techniques try to provide some effective tools or schemes to protect the ad hoc routing services from all kinds of attacks.

Security Solutions in the Mobile Ad Hoc Networks:

We examine the security solutions in mobile ad hoc networks in this part. We start by examining the primary security requirements for mobile ad hoc networks, which serve as a roadmap for resolving security concerns in these networks. Next, we highlight the different kinds of attacks that primarily target mobile ad hoc networks. We examine various security approaches that can partially address the security issues in mobile ad hoc networks based on these attack types.

6.Conclusions

We attempt to examine the security flaws in mobile ad hoc networks in this survey study, since they could be a major hindrance to their functionality. Mobile ad hoc networks are more vulnerable to several security threats, including information leakage, intrusion, and denial of service attacks, because of its open media and mobility. Because of this, mobile ad hoc networks have far greater security requirements than typical wired networks. First, we provide a quick overview of the fundamental features of mobile ad hoc networks.

The rise of mobile ad hoc networks is fueled by the growing requirement for network users to connect to the outside world at any time and from any location, as a result of the pervasive computing idea. However, despite the convenience that mobile ad hoc networks have provided, there are growing security risks associated with them that require adequate attention. We then go over a few common and risky vulnerabilities in mobile ad hoc networks, the majority of which are brought on by the networks' inherent features, including mobility, dynamic topology, open media, and low battery life.

Finding some efficient security solutions to shield the mobile ad hoc network from various security threats has become essential due to the prevalence of these vulnerabilities. Lastly, we present the most recent security fixes for mobile ad hoc networks. The security criteria in mobile ad hoc networks are discussed, and this serves as a guide for security-related research projects in this field. The primary attack types that pose a danger to the existing mobile ad hoc networks are then discussed. Finally, we go over a number of security strategies that can be used to defend mobile ad hoc networks against both internal and external security risks. The survey also reveals certain areas that may be investigated further in the future, such as areas where intrusion detection methods could be further enhanced. We shall make an effort to delve further into this field of study.

References

1. Royer E.M. and Toh C.K.(1999) IEEE Personal communiation. [11] Jyoti Raju and J.J. Garcia-Luna-Aceves,"A comparison of on-Demand and Table-Driven Routing fo rAd Hoc Wireless network",inProceeding of IEEE ICC,June 2000.
2. C.Perkins and E.Royer ,"ad hoc on demand distance vector routing," 2 nd IEEE wksp. Mobile comp. sys. And Apps.,1999
3. G.Johnson and D.Maltz(1996).,"Dynamic source routing in ad hoc wireless network ,"mobile
4. computing T.Imielinski and H.Korht , PP.153-81.kluwer.
5. Y-C. Hu, A.Perring and D.Johnson(2006),"Wormhole attacks in wirelessnetworks," IEEE JSAC,vol.24,no.2
6. S.Desilva, and R.V. boppana,"Mitigating malicious control packet floods in ad hoc network," Proc.IEEE wireless commun. And networking conf., new orleans,LA, 2005.

7. H.Yang,H.Luo,F.Ye,S.Lu,L.Zhang,"security in mobile ad hoc network:challenges and solutions," In Proc.IEE wireless communication, UCLA,Los Angeles,CA,USA;volume-11,pages 38-47.
8. Ping Yi, Yue W and futai zou and ning liu(2010),"A survey on security in wireless mesh network",Proc. Of IETE Technical review, vol,27,issue 1.
9. B.Wu,J.Chen,J.Wu,M.Cardei,"A survey of attack and countersmeasures in mobile ad hoc networks," department of computer science and engineering,floridaatlanticuniversity
10. H.Deng,W.Li.,Agrawal ,D.P(2002),"routing security in wireless ad hoc networks,"cincinnati univ.,OH,USA; IEEE communications magazine, volume:40,pages(5):70-75.
11. Abhay kumar rai,rajiv ranjan tewari , saurabh kant upadhay ," different types of attacks on integrated MANET-Internet communication,"international journal of computer science and security(IJCSS)volume(4):issue(3).
12. Pradip m. Jawandhiya,mangesh m. ghonge, dr.m.s.ali ,"A survey of mobile ad hoc network attacks,"international journal of engineering science and technology vol.2(9),2010,4063-4071.
13. B. Bellur and R. G. Ogier(1999)," A reliable, efficient Topology broadcast protocol for dynamic
14. Networks", In Proceedings of the Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom), pages 178–186.
15. M. Blaze, J. Feigenbaum, J. Ioannidis, and Keromytis. The Keynote trust-management System Version 2. Internet RFC 2704,September 1999.
16. E. Bonabeau, M. Dorigo, and G. Theraulaz. Swarm ntelligence: From Natural to Artificial Systems. SFI Studies in the Sciences of Complexity. Oxford University Press, July 1999.
17. S. Buchegger and J.-Y. Le Boudec(2002)," Performance analysis of the CONFIDANT Protocol", In Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), pages 226–236.
18. L. Butty´an and J.-P. Hubaux. Rational exchange –a formal model based on game Theory. In Proceedings of the 2nd International Workshop on Electronic Commerce (WELCOM), November 2001.
19. L. Butty´an and J.-P. Hubaux. Stimulating Cooperation in self-organizing mobile ad hoc Networks. ACM/ Kluge Mobile Networks and Applications (MONET), to appear 2002.
20. L. Butty´an, J.-P. Hubaux, and S. Cˇ apkun. A Formal analysis of Syverson's rational exchange protocol.In Proceedings of the 15th IEEE Computer Security Foundations Workshop (CSFW), June 2002.
21. S. Cˇ apkun, L. Buttya´n, and J.-P. Hubaux. Small worlds in security systems: an analysis of the PGP certificate graph. In Proceedings of the ACM New Security Paradigms Workshop , 2002.
22. C. Castelluccia and G. Montenegro. Protecting AODVng against impersonation attacks. ACM Mobile Computing and Communications Review, July 2002.
23. M. Corner and B. Noble. Zero-interaction authentication. In Proceedings of the 8th ACM International Conference on Mobile Computing and Networking (MobiCom), September 2002.
24. C. Ellison and al. SPKI certificate theory. Internet RFC 2693, September 1999.
25. Y.-C. Hu, D. B. Johnson, and A. Perrig. Secure Efficient distance vector routing in mobile Wireless ad hoc networks. In Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), June 2002.
26. H. Goto, Y. Hasegawa, and M. Tanaka(2007),"Efficient Scheduling Focusing on the Duality of MPL Representatives," Proc. IEEE Symp. Computational Intelligence in Scheduling, IEEE Press, pp. 57-64.