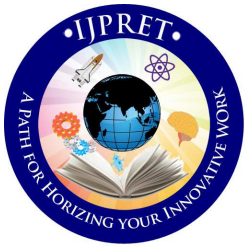
Research Article *ISSN: 2319-507X*
Yogita Lakade, IJPRET, 2013; Volume 1(8):333-338 *IJPRET*



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURITY ISSUES AND CHALLENGES IN AD-HOC NETWORKS

YOGITA P. LAKADE, PROF. S.S. ASOLE

1. M.E., Babasaheb Naik College of Engineering,Pusad Department Computer Science & Engineering.
2. Asst. Prof., Babasaheb Naik College of Engineering,Pusad Department Computer Science & Engineering.

Accepted Date:
27/02/2013
Publish Date:
01/04/2013

Keywords
Ad Hoc Network,
Security,
Wireless Network,
Topology.

Corresponding Author
Ms. Yogita P. Lakade

Abstract

An ad hoc network is self-configuring network of wireless link connecting node these may be router and hosts. These node communicate directly with each other and without the aid of access point and have dynamic topology, no fixed infrastructure. In the last years, ad hoc networks have received special attention because of their advantages: they can be deployed easily and cheaply, as they don't need pre-existing infrastructure, they are autonomous (self-configured and self-maintained).but we know that Security has always been an essential issue in wired and wireless networks. And in Ad hoc network are highly vulnerable to security attack and dealing with this is one of the main challenge of developer. The main reasons for this difficulty are it shared broadcast radio channel, in securing operating environment, lack of central authority, lack of association among limited availability of resources and physical vulnerability. This paper analyzes security challenges in wireless networks and summarizes key issues that need be solved for achieving security in an ad hoc network

INTRODUCTION

Ad hoc networks are new paradigm of networks offering unrestricted mobility without any underlying infrastructure. An ad hoc network is a collection of autonomous nodes or terminals that communicate with each other by forming a multi hop radio network and maintaining connectivity in a decentralized manner. In the ad hoc networks, there is no fixed infrastructure such as base station or mobile switching. Since the nodes communicate over wireless links, they have to contend with the effects of radio communication, such as noise, fading, and interference. In addition, the links typically have less bandwidth than in a wired network. Each node in a wireless ad hoc network functions as both a host and a router, and the control of the network is distributed among the nodes. The network topology is in general dynamic, because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes.

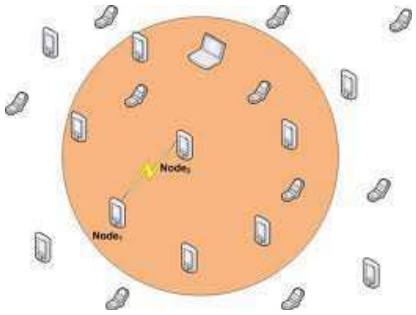


Figure 1: Example of an ad hoc network

SECURITY ISSUES

Ad Hoc Networks Ad hoc networks comprise a special subset of wirelessnetworks since they do not require the existenceof a centralized message-passing device. Simple wireless networks require the existence of staticbase stations, which are responsible for routing messages to and from mobile nodes within the specified transmission area. Ad hoc networks, on the other hand, do not require the existence of any device other than two or more nodes willing to cooperatively form a network. Instead of relying on a wired base station to coordinate the flow of messages to each node, individual nodes form their own network and forward packets to and from each other. This adaptive behavior allows a network to be quickly formed even under the most adverse conditions.

SECURITY REQUIREMENTS:

CONFIDENTIALITY:

Data transmitted in the network must be protected against unauthorized parties. As the ad hoc network architecture is open, it is very easy for anyone with appropriate devices and knowledge of network topology and protocols to connect to it and to gain access to the transmissions. One way to achieve confidentiality is by using encryption mechanisms.

DATA INTEGRITY:

Data transmissions in the network must not be altered or destroyed in any way. In MANETs the malicious users can modify, delete and resend data pretty easily due to wireless medium vulnerability**.**

AUTHENTICATION:

There are two aspects: message authentication (message content is valid) and node authentication (every node is who he claims to be). In wired networks and infrastructure based wireless networks, this is usually done by a central authority, but in ad hoc networks implementing such a mechanism is very challenging.

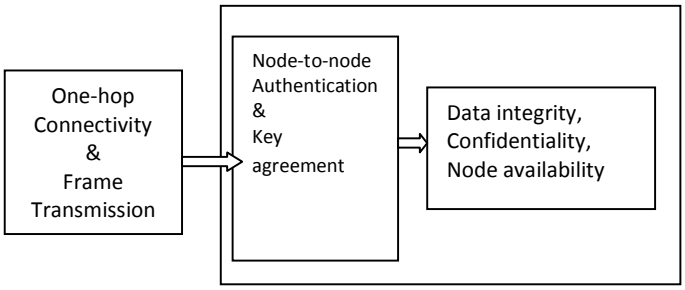
NONREPUDIATION:

This means that a sender of a message cannot deny having send it. This function intends to make possible intrusion detection and messageinjection. Routingand authentication algorithms usually rely on it.

AVAILABILITY:

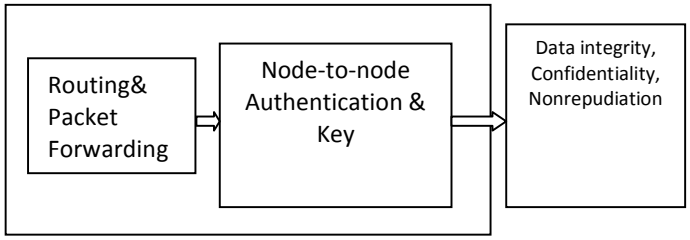
This is the most important requirement for a network and means keeping the network service and resources available to legitimate users. If this function is not granted, there is no network to talk about. In ad hoc networks, there are supplementary problems to overcome, due to node mobility and to network dynamics.

SECURITY APPROACH:-



Presecure session detection

Postsecure session



Prevention/reaction

Fig 2 Security Approach

Main link layer operations related to ad hoc networking are one-hop connectivity and frame transmission, where protocols maintain connectivity between neighboring nodes and ensurethe correctness of frames transferred. The main network operations related to ad hoc networking are routing and data packetforwarding, where protocols exchange routing data between nodes and maintain routing states at each node accordingly As illustrated in Figure these operations comprise link security and network security mechanisms that integrate security in presecureand postsecuresessions.

Advanced Security Approach in Authentication: Two Phase

PRESECURE PHASE: In this phase the node identification procedure assumes that the secret is known to the verifying node, and this secret is used to verify the response. Here the node authentication procedure attempts to determine the true identity of the communicating nodes through challenge–response protocols based on symmetric-key techniques.

B←X1: r1 (1)

B → X1: Ek(r1 , r2, B) , (2)

B ← X1: Ek(r2 , r1) , (3)

E is a symmetric encryption algorithm and r1 and r2 are randomnumbers.

POSTSECURE PHASE: In thepostsecure phase (also referred to as the second phase) of the authentication, the secret is not known to the verifying node. Here the authentication procedure seeks again the identities ofthe communicatingnodes through challenge–response protocols based on public key techniques where it can be applied before private information is exchanged between communicating nodes.

X1 →C: PC(r1, X1) , (4)

X1 ←C: PX1(r1 , r2) , (5)

X1 →C :r2 , (6)

P is a public key encryption algorithm and r1 and r2 are random numbers**.**

Table 1 Timing analysis of encryption algorithms for specific key size

Cryptographic algorithms	Key length(bits)ms	Encryption(500bit)ms	Decryption(500bit)ms
AES	128	20	23
MD5-MAC	128	10	10
RSA (with CRT)	2048	50	120
ECC Menezes–Vanstone	224	72	68

CONCLUSION:-

In this paper, security relevant issues within ad hoc networks are identified. A brief introduction about key issues and challenges provides the decomposition of whole security issue within ad hoc networking. Significant usages of ad hoc network leverage on the well-defined security architecture, where security aspects like confidentiality, Integrity and availability, privacy are addressed properly. and we explored integrated cryptographic mechanisms in phases that helped to design multiple lines of authentication defense and further protect ad hoc networks against malicious attacks. once the authentication and key management infrastructure is in place, data confidentiality and integrity issues can be tackled by using existing and efficient symmetric algorithms since there is no need to develop any special integrity and encryption algorithms for ad hoc networks.

REFERENCES:-

1. NikosKomninos, Dimitrios D. vergados and Christos Douligeris: security for Ad hoc netwoks.

2. C. Perkins: Ad Hoc Networking (Addison-Wesley,Boston, USA 2000)

3. 3 .L. Zhou, Z.J.Haas: Securing ad hoc networks, IEEENetw. Mag. 13(6), 24–30 (1999)

4. A.J. Menezes, S.A. Vanstone, P.C. Van Oorschot:Handbook of Applied Cryptography (CRC Press,Boca Raton 2004)

5. 1. S. Basagni et al., eds., Mobile Ad Hoc Networking,IEEE Press, 2003.

6. K. V. Mangipudi, R. S. Katti, and H. Fu, \Authentication and key agreement protocols preservinganonymity," International Journal of Network Security, vol. 3, no. 3, pp. 259270, 2006.

7. Y. Hu, A. Perrig, D. Johnson, "Rushing Attacks and Defensein Wireless Ad Hoc Network".

8. Lidong Zhou, Zygmunt J. Hass, "Securing Ad Hoc Networks",IEEE Networks Special Issue on Network Security,November/December 1999.

9. Shuyao Yu, Youkun Zhang, Chuck Song, and Kai Chen. Security architecture for Mobile Ad Hoc Networks

10. Clarke, Roger. Conventional Public Key Infrastructure: An Artifact Ill-Fitted to the Needs of the Information Society. Canberra : Clarke, 2000, accessed 12 Oct. 2004.