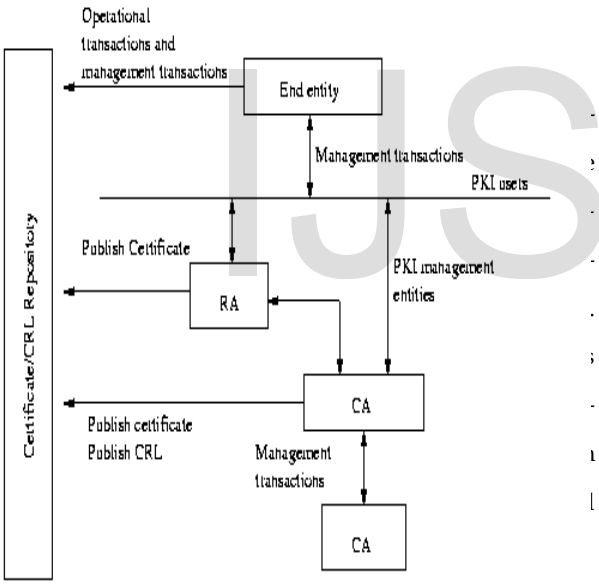
Study of **Wireless Ad-Hoc Networks**

Gurvail Singh, Aarti, Harwant Singh
Department of Computer Science & Engineering, Lovely Professional University (PUNJAB), INDIA
Sandhusmile36@gmail.com
Department of Computer Science & Engineering, Lovely Professional University (PUNJAB), INDIA
Aartihans07@gmail.com
Asst. Prof., Department of Computer Science & Engineering, Lovely Professional University (PUNJAB), INDIA
hs.arri@lpu.co.in

Abstract— *-This paper proposes a basic scheme for understanding the fundamentals of wireless ad-hoc networks and Cryptographic Algorithms t. There are two type of attacks in network. The main* Task is to understand the ad-hoc network for creating a network in which a intrusion node can be detected and a secure network can be prepare.
.

Index Terms— Security Threats, Mobile Ad Hoc Network, Wireless Network, Cryptographic Algorithms.

1 INTRODUCTION



An a
ized adn
nodes an
tablish th
tive and
The othe
dissertati
vide the
unauthor
provide t

1.1 Background and Motivation

MANET is having excellent attention because it is self-configure and maintained network. However in research it is having a friendly and cooperative environment with the problem of multi hop routing and wireless channel access and security is the major concern. In mobile adhoc network when nodes are in free conditions then there is a chance when an unauthorized node can be a part of the network. That unauthorized node can be a attack on the network and leek the necessary information from the network and disturb the routing process. To authorize the all nodes in the wireless network the CA is introduced in the network.

1.2 Security Threats

There are two type of attacks in network:

Active Attack: Active attacks are those in which the third person can change the content of message and send to the receiver. The four process comes in active attacks are message modification, denial-of-service, masquerading and replay.

- **Masquerading**
- **Replay**
- **Message modification**
- **Denial-of-service**

Passive Attack: In passive attack only the third party can see the content of message but cannot be change it. There are two type of passive attack which is given below.

- **Eavesdropping**
- **Traffic analysis**

1.3 Mobile Ad Hoc Network

The nodes are mobile and this is a dynamic technology so the changes can be made at any situation. But the routing protocol is not suited to dynamic environment. This network does not contain any fixed router; hence each node can be a router.

1.4 Wireless Network

Mobile wireless networks are having two type of variations [7].

1.4.1. Infrastructure Network: The base stations work as a bridge in this fixed and wired gateways network. Cellular-phone networks are an example of this wireless network. When the phone is out of range of one base-station and into range of another, a "hand-off". The "hand-off" should be fast enough to be seamless for the user of the network.

1.4.2. Infrastructure less Network: an infrastructure less network is only for participating nodes. This temporary network perform peer-level multi-hopping which make the base for ad hoc networks for the mobile nodes.

1.4.3 Another Classification Of Wireless Networks:

1.4.3.1. Fixed Wireless Network: wireless channels to make communication with fixed wireless network, An example of a wireless network which is given below:

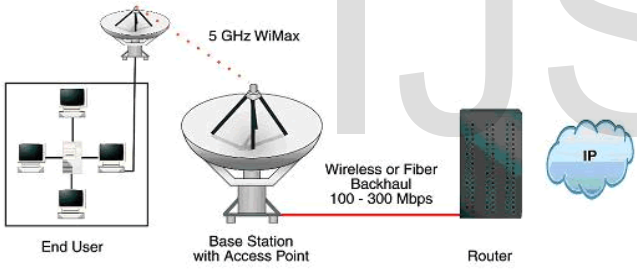


Figure (1.2) Fixed Wireless Network

1.4.3.2. Wireless Network with Fixed Access Points: hosts node use wireless channels to make connection with fixed access points, These access points are the routers for those mobile hosts, to generate a mobile network having fixed access points.

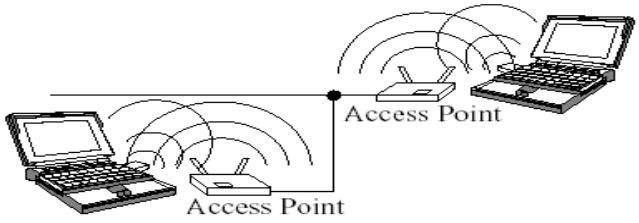


Figure (1.3) Wireless Network And Access Points

1.5 Applications of Mobile Ad Hoc Network

The MANET's having the different applications in various services which make it popular.

S. No	Applications	Possible services and scenarios
1.	Tactical networks	• Military operations and communication.
2.	Sensor networks	• Home applications •Environmental applications • Remote sensors for weather, remote sensors and activities. • BAN
3.	Accidental and Emergency Services	• Search work. • Recovery of disaster. •Relocate the fixed infrastructure (environmental disasters). • Retrieval of patient data.
4.	Commercial and civilian environment	• E-Commerce • Business: database access. •Local network for road guidance. • Sports and shopping malls.
5.	Home and enterprise Networking	• PAN. • Conferences.
6.	Educational Application	• Setup conference rooms
7.	Entertainment	• Multi-user games. • Outdoor gaming access on internet.
8.	Location aware Services	• Follow-on services. • Information facility: services (printer, fax) • Touristic record.
9.	Coverage Area extension	•Extending cellular network access limit.

Table (1.1) Applications of Ad Hoc Network

1.6 The Purpose Of Cryptography In Manet's

Cryptography is the science which performs encryption and de-cryption of on plain text. The security is depend s upon two thing the cryptographic algorithm and key. In symmetric key the en-cryption and decryption is performed with the help of one key. But in the case of asymmetric key the encryption and decryption is performed with two key. Character string feature is used for making password that map the plain text with cipher text.

Within the context of any application-to-application communica-tion, the some security requirements are given below:

- Authentication.
- Privacy.
- Integrity.
- Non-repudiation.

Three cryptographic schemes:

1. Secret key cryptography
2. Public-key cryptography
3. Hash functions

1.7 Types of Cryptographic Algorithms

The Figure (1.4) described all three algorithms.

- Secret Key Cryptography
- Public Key Cryptography
- Hash Function

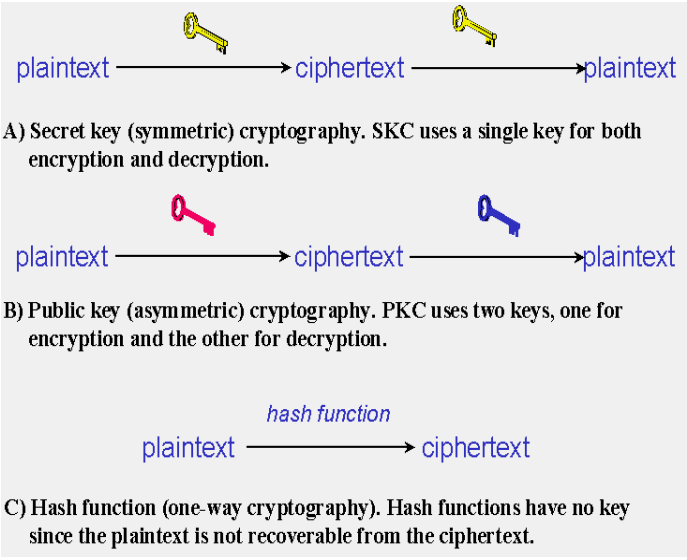


Figure (1.4) Types of Cryptography

1.7. 1 Secret Key Cryptography

Secret key cryptography is also known as symmetric key cryptography because both the sender and receiver use the same key to encrypt and decrypt the data. In first situation the sender use the same secret key and perform the encryption on the plain text then on the receiver side the receiver receive the encrypted data and decrypt it with the help of same key. Both the side use the single secret key.

stream ciphers or block cipher are the part of secret key cryptog-raphy. Stream ciphers work on a single bit at a time. A block ci-pher encrypts a block of data with the same key.

1.7.2 Public-Key Cryptography

Public key cryptography usually uses the two key for encryption and decryption of the data. in first step when the encryption is performed then one key is used on the plan text to convert it cypertext and when the decryption is performed then other key is used .no matter which key is use first for encryption or decryption

1.7.3 Hash Functions

Hash functions are also known as message digests and one-way encryption. Hash function is used to measure the integrity of file and to make a password of an application. In hash function a fixed length of value is applied on a value which is calculated during the process of encryption and decryption

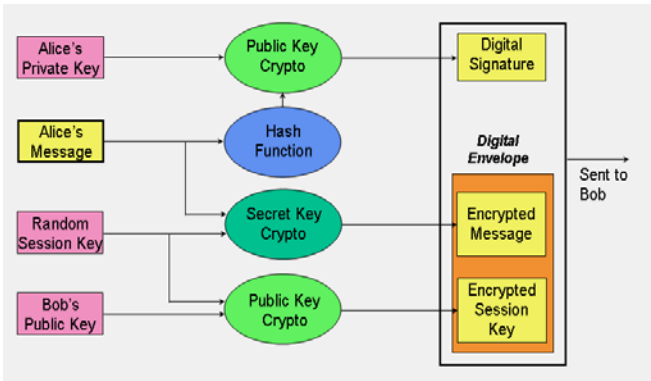


Figure (1.5): Three Cryptographic Techniques For Secure Com-munication.

1.8 PKI (Public Key Infrastructure)

PKI is a security mechanism which provides security in mobile network. In wireless network all the nodes are mobile. Multiple hoping technique is used when a base station provide a range to a cellular phone. When all nodes are mobile then there is chance when a third party insert a node in a network which can steal the information and create the disturbance in the network. For preserving the network PKI is used which provide the authentication to the network. A technology known as CA provide the authentication certificate to each node so that when a node with no certification is come under the network then the network automatically reject that particular node. This provide security to our network which is the main concern of this dissertation.

2. Conclusion

In mobile ad hoc network there is a chance when an authorized node a part of the network, that unauthorized node can produce the disturbance in network so to overcome this problem we will introduce the PKI in our work that provide a authentication certificate to each node that make the network more secure and the third party cannot make any type of interrupt in the network. To introduced the security matter in this work the CA will provide the authentification certificate to each node so that the when the node moves to the other node there is node a fraudulent node in the network that steal the information. In the current work we have proposed the theory for Different attacks over the adhoc network and PKI security model and we have shown its different variant of the security models. In future we will implement these models and simulate it to show the impact of certificate authority (PKI)

3. REFERENCES:

[1] Distributed CA-based PKI for Mobile Ad Hoc Networks Using Elliptic Curve Cryptography by Charikleia Zouridaki, Brian L. Mark, Kris Gaj, Roshan K. Thomas

[2] Security in wireless ad hoc networks by amitabh mishra & ketan M.nandkar

[3] Nitiket Mhala and Nilesh P Bobade, " Performance Evaluation of Adhoc On Demand Distance Vector in Manets with varying Network size using NS-2 Simulation", International Journal on Computer Science and Engineering (IJCSE) Volume 02 , August, 2010.

[4] Gopinath Ganapathy and Geetha Jayakumar, "Performance Comparison of Mobile Ad-hoc Network Routing Protocol", International Journal of Computer Science and Network Security (IJCSNS), Volume 07, November 2007.

[5] Yanchao Zhang, Member, IEEE, Wei Liu, Wenjing Lou and Yuguang Fang, "Securing Mobile Ad Hoc Networks with Certificateless Public Keys", IEEE Transactions on Dependable and Secure Computing,Volume 03, OCT-DEC 2006.

[6] Papadimitratos Panagiotis and J.Haas Zygmunt "Secure Data Communication in Mobile Ad Hoc Networks" IEEE Journal On Selected Areas In Communications Vol 24 No2. February 2006.

[9] Svein Johan Knapskog, "New Cryptographic Primitives (Plenary Lecture)",7th Computer Information System and Industrial Management Applications, IEEE 2008.

[10] Yue Ai and Fuwen Pang, "Improved PKI Solution for Mobile Ad Hoc Networks", IEEE 2010.

[[12] G Varaprasad and P. Venkataram, "The Analysis of Secure Routing in Mobile Ad Hoc Network", International Conference on Computational Intelligence and Multimedia Applications, IEEE 2007.

[13] Maqsood Razi, Jawaid Quamar, "A Hybrid Cryptography Model for Managing Security in Dynamic Topology of MANET" IEEE 2008.

[14] Alberto Ferrante and Antonio Vincenzo Taddeo, "A Security Service Protocol for MANETs", IEEE 2009.

[17] Manali J Dubal, Mahesh T R and Pinaki A Ghosh, "Design of New Security Algorithm, Using Hybrid Cryptography Architecture", IEEE 2011.