Volume 4, Issue 7, July 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secure Communication over Insecure Open Medium for an Infrastructure less Ad-Hoc Networks

K. Nirmala[1], P. Penchalaiah[2], D. V Subba Rao[3]

[1]Research Scholar, Department of Computer Science and Engineering, S.V University, Tirupathi, A. P., India

[2]Research Scholar, Department of Computer Science, V.S University, Nellore, A. P., India

[3]Professor and HOD of Department of Computer Science & Engineering, S.V University, Tirupathi, A. P., India

Abstract - A mobile ad-hoc network (MANET) is collection of portable devices or PDA's with conjunction with mobile communication, which is designed to communicate to one or more nodes. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure called as infrastructure less and central coordination. Since the MANET is exposed to open world where there is limited or no restrictions to join in the network to the nodes. MANNETs are designed only to provide correct routing and have ability to adjust or self configure to their dynamic changing condition. So MANET is more venerable to threats by its behavior. Security is an important issue for ad hoc networks, especially for those security-sensitive applications. To secure an ad hoc network there must be an efficient cryptographic system. In this paper, we propose a cryptosystem model to provide security between nodes.

Keywords: Ad-hoc Network, Cryptography, Encryption, Decryption, Commutative Key Exchange.

I. INTRODUCTION

In recent years mobile ad hoc networks (MANETs) became an emerging technology and have received tremendous attention because of their self-configuration and self-maintenance capabilities. A MANET is a system of wireless is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others nodes helps to route their packets. Security has become a primary concern to provide protected communication between mobile nodes in an insecure environment.

Unlike wired line networks, the unique characteristics of mobile ad hoc networks impose a number of challenges to the security design. Flexibility in MANET offers to establish communication without any fix base station. But this flexibility such as dynamic topology, open medium and distributed cooperation are reason to be venerability in mobile ad-hoc network.

Problem Definition

One of the characteristics of MANET is Multi hop routing, when a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes. Here is the problem what happens if the intermediate nodes (compromised node) try to interpret the information before forwarding? What happens if the information is forwarded to third party node? The necessity of information privacy leads to the development of new methods and techniques for secure data transmission. So here cryptography places an important role even the information received by unintentional node it should not be readily useful to the node.

II. SECURITY ATTACK IN MANETS

There are a variety of attacks that target the weakness of MANET due to of its flexible features. For instance, routing messages are vital component in a network communications, where each packet needs to be passed through various neighbor intermediate nodes, which gives a path to the packet to traverse from a source to the destination. Here are the case where malicious node attacks by not following the specifications of the routing protocols. More sophisticated and subtle routing attacks have been identified in recent published papers. Currently routing security is one of the hottest research areas in MANET.

Attacks

The attacks in MANET can roughly be classified into two major categories, namely *passive attacks* and *active attacks*. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. The attacks again can also be classified into two categories, namely *external attacks* and *internal attacks*, according the domain of the attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights.

To secure an ad hoc network, the following attributes are important to be considered: *availability*, *confidentiality*, *integrity*, *authentication*, and *non-repudiation*. But in this paper we are presenting only about *confidentiality.*

Confidentiality

Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical information, requires confidentiality. Leakage of such information to opponents could create panic situations.

III. KEY MANAGEMENT SERVICE

. Key management is problematic for Ad-hoc networks because MANETs are infrastructure less and lack of central coordination. So here we can't use Public key infrastructure as a key management service for Ad-hoc networks. There is the following alternative for key management.

1. Key exchange between nodes.
2. Self key managing by listening and updating.

Key exchange between nodes

The nodes that are participating in the communication must agree up on a security association before the actual communication commences (Ref Fig 1.0). Here security association means set of rules or policies for exchanging a code word securely between the nodes.

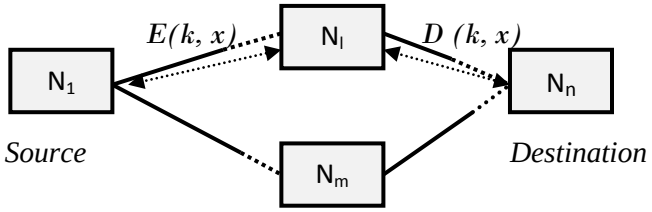


Fig: 1.0 Key Exchanging

In Fig 1.0 N_1 and N_n (N – node)established an association via N_i intermediate node. In general this model uses commutative function for encryption and decryption.

Self key managing by listening and updating

In this method each node must have a unique identification (ID) and manages key database. Initially it contains recently communicated nodes ID and Keys. Gradually by listening to network nodes or polling to other nodes each node updates its key database.

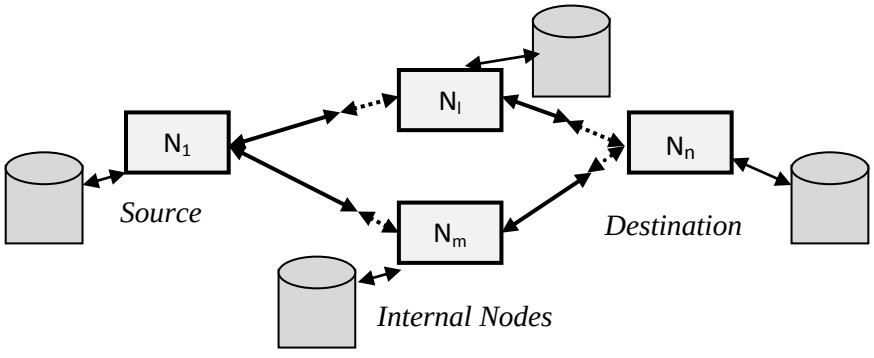


Fig: 1.1 Self Key Managing

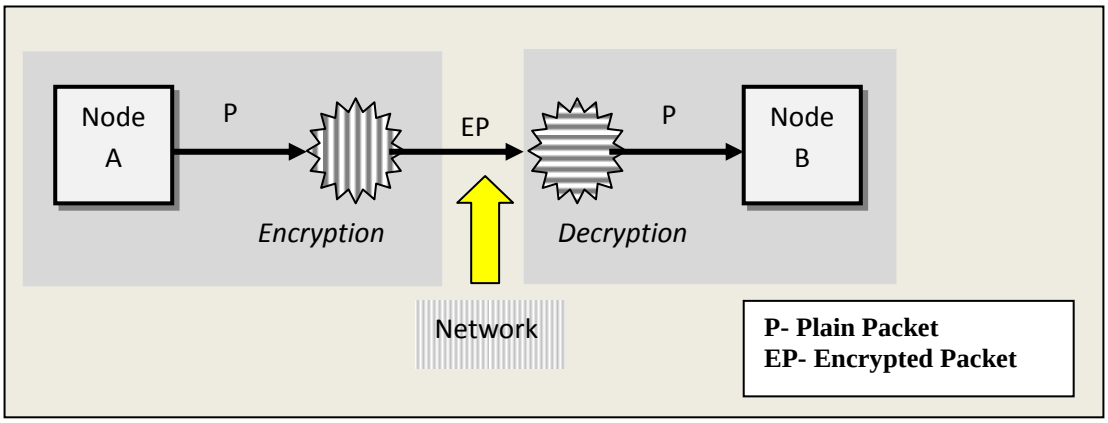
Most of the solutions for secure routing and data forwarding rely on cryptography. *Cryptography* is the practice and study of hiding secret information by encryption. *Encryption* is a process of conversion of data into a unintelligence form, called a cipher-text. *Decryption* is just inverse process, in other words, converting from unintelligible cipher-text back to plaintext. Modern cryptography intersects the disciplines of mathematics and computer science. Cryptographic techniques are needed for confidentiality (privacy) and authentication of digital data. There are two types of cryptic algorithms used in cryptography, namely *Symmetric-Key Encryption* (also known as single-key encryption, one-key encryption) and *Asymmetric Encryption* (Public Key Encryption).

Ad-hoc network can employ any key management service that entertains the Ad-hoc network flexible characteristics. Once both the nodes agreed on any association, the following procedure (Fig 1.2) can apply for secure communication. For better understandability here we are using shamir's commutative key exchanging algorithm.

Procedure:

1. Establish a security association between the nodes by using Key Exchanging Algorithm (Shamir's. commutative key exchanging).
2. Use any strong cipher like Permutation cipher, Vigenere cipher for encryption and decryption. Both nodes must follow same cipher.
3. At source, encrypt the message packet M using associated cipher E(M) and send it to destination.
4. At destination decrypt the encrypted message D (E(M)).

.



V. CONCLUSION

In this paper, we have analyzed the security threats an ad hoc network faces and presented a security model for secure packet routing, which maintains confidentiality even a compromised node receives the packet. On the other hand, the security-sensitive applications of ad hoc networks require high degree of security. Therefore, security mechanisms are indispensable for ad hoc networks.

REFERENCES

[1] [1] Aarti and Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", IJARCSSE, Vol 3, Issue 5, May 2013.

[2] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, And Lixia Zhang, "Security In Mobile Ad Hoc Networks: Challenges And Solutions" IEEE Wireless Communications, February 2004.

[3] Jangra1,A. Goel,N. Priyanka and Bhati,K. – Security Aspects in Mobile Ad Hoc Networks(MANETs): A BigPicture, International Journal of Electronics Engineering, pp. 189-196, 2010.

[4] P.Penchalaiah , K. Ramesh Reddy "Efficient and Secure Encryption Schema based on Random bits (Rbits)" International Journal of Advanced Research in Computer Science and Software Engineering" Volume 3, Issue 11, November 2013 pp. 1026-1032.

[5] Y. Hu and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing. IEEESecurity & Privacy, pp. 28-39, 2004.

[6] W. Stallings, Wireless Communication and Networks, Pearson Education, 2002.

[7] Y. Hu, A. Perrig, and D. Johnson, Ariadne: A Secure On-Demand Routing for Ad Hoc Networks. Proc. of MobiCom 2002, Atlanta,2002**.**

