Review Paper on Mobile Ad-hoc Networks

Hiral Vegda
Lecturer, School of Computer Studies
Ahmedabad University,
Ahmedabad, Gujarat,
India

Nimesh Modi,PhD
I/C HOD, Cyber Security Program,
Department of CS,
Hemchandracharya North Gujarat University, Patan,
Gujarat, India

ABSTRACT

Mobile Ad-hoc networks have been broadly research for many years. Ad-hoc system may be an accumulation from claiming hubs that is joined through a remote medium framing quickly evolving topologies. The infrastructure takes away as well as the dynamic life of these networks anxiety newborn become hard of networking strategies route for staying implemented into orderliness near give capable end-to-end communication. Mobile Ad-hoc Network (MANET) is special types of mobile wireless network where the groups of mobile devices form a temporary network without any kind of an infrastructure. It is very useful due to its self maintenance, self organizing and by reason of mobility of wireless communication. In mobile ad-hoc network there are so many attacks which reduced the performance of network. MANET works under no fixed infrastructure in which every node works likes a router that stores and forwards packet to final destination. Due to its dynamic topology, MANET is anywhere, anytime. Since nearby are as there are limited resources in MANET so it faces many problems such as security, limited bandwidth, range and power constraints. This paper examine at different systems on manage congestion control, security issues, separate layers attacks, routing protocols and challenges that are faced by MANET.

General Terms

Mobile Ad-hoc Networks

Keywords

MANET, Security, RSA Algorithm, DES Algorithm

1. INTRODUCTION

Mobile ad-hoc network is a way of communication, among different portable devices, without offering a centralized device. There is no need of any access point in mobile ad-hoc network. It is the beauty of mobile ad hoc network that mobile nodes communicate with different nodes in the absence of any fixed or central infrastructure, this property of MANET makes it different and unique among all other networks [9].

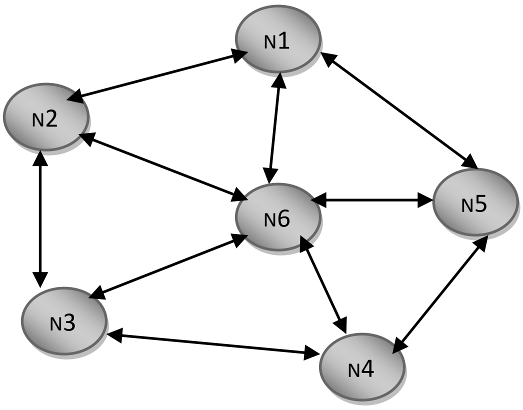

Fig 1: Mobile ad-hoc network architecture [1]

Mobile ad hoc network (MANET) is a collection of mobile nodes connected with wireless links. Deployment of MANET does not require any fixed existing infrastructure or any centralized administrator. There is no need of any static infrastructure or base station for communication. As all the nodes in a MANET are wireless in nature, they are free to move randomly. Thus the network topology changes frequently[3]. In mobile communication topologies are dynamically created due to the ad hoc nature of the network infrastructure and mobility. MANET architecture shown as in Figure 1. MANETs have some limitations also such as unreliable communication medium, dynamic topology, limited bandwidth, battery power and lifetime etc. Routing is also a challenging task in a MANET. It is more vulnerable to route packets in MANET as compared to wired networks. Security in MANET is also a critical issue that is still a largely unexplored area. Since nodes use the open, shared radio medium in a potentially insecure environment, they are highly prone to malicious attacks, such as denial of service (DoS). Lack of any centralized network management or certification authority makes the network very much vulnerable to infiltration, eavesdropping, interference etc. Many protocols are designed to provide security in MANETs. These protocols include authentication, non-repudiation and message integrity as part of security policy for the ad hoc environment.

Some of them also provides secure routing which helps to choose the most trustworthy and stable routes. But none of these protocols provide an efficient way of certificate exchange for authentication [3].

2. SECURITY IN MANET

Security of MANET is one of the major concerns with respect to support a safe and healthy communication among communicating nodes in an unfriendly environment. No infrastructure is followed by communicating nodes in ad hoc network, instead they organize themselves dynamically which results in emergence of new challenges for the basic security in applied architecture. Due to this sensitive infrastructure MANET can be directly attacked by hackers. By violating network confidentiality, eavesdroppers can approach secret information [9].Furthermore, as mobile ad hoc networks are normally designed for some particular environment, security solutions designed for wired network may not be suitable for them. In contrast with traditional networks, where dedicated routers are placed to perform the basic functionality of network, MANET relies on respective nodes in order to achieve the required connection among nodes. All basic functions like routing, data forwarding and network management are performed by all alive nodes. Therefore, every node must be ready for encounters every time it desires to communicate. Encounters by compromised nodes are much more destructive because detection of compromised nodes is hard to achieve. Providing the essential security services, for instance; confidentiality, availability, integrity, and authentication to mobile users, is the utmost aim of security solutions in MANET [9].

3. SECURITY CHALLENGES [9]

Challenges and opportunities in achieving the security goals are two main features of MANET. The security factor in adhoc networks is very essential to fulfill the basic functions like packet forwarding and routes etc. The use of ad hoc networks is now increasing especially in sensitive areas like emergency, military etc., where security is essentially required in order to protect network from attacks by malicious nodes. Because of dynamic nature of ad hoc network, a trusted relationship among nodes is hard to derive. As there are various types of attacks that can severely harm the MANET, so it is needed in security mechanisms to adjust and manage on-the-fly changes. Network operations can easily be affected if counter steps are not embedded into their design. As MANET holds dynamic nature so it does not have any centralized or fixed structure, all nodes in such networks are not in direct transmission range for each other. One may not accept the present infrastructure. Setting up an infrastructure in this situation is not useful in terms of expenses and time consuming. On that account, supporting the required network services and connectivity appears a real issue. In a MANET mobile nodes exchange variable number of datagram along different paths build up by many routing algorithms in order to communicate with each other in reliable manner, here, reliability is the ability to provide high delivery data ratio and send most of the messages in spite of links breaking the paths or capacity overflows caused by congested nodes [9].

4. RSA APPROACH

RSA stands for the name of the three researchers who designed it. Public key are being utilized as a part of RSA for secure transmission of information or data. The required key for encrypting the data is public and for decrypting the data key is private as shown in figure. Factorization of two major prime numbers is utilized as a part of RSA [4].

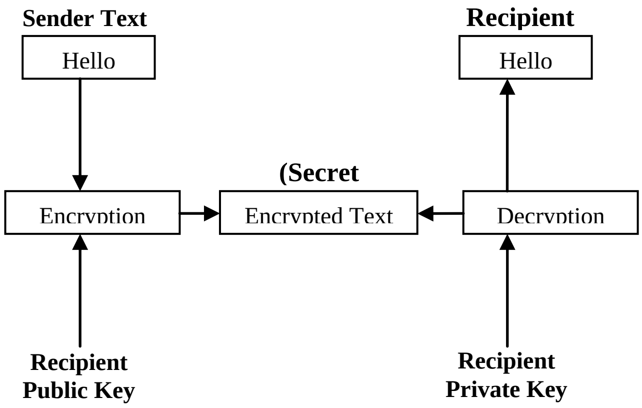

Fig. 2. Working of RSA[4]

5. MD5 ALGORITHM

The MD5, message-digest algorithm is a widely cryptographic hash function producing a 128 bit hash value, typically expressed as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of security applications. It is also commonly used to check data integrity. MD5 message-digest algorithm takes a message of arbitrary length as input and produces a 128 bit "message digest" as output. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) Key under a public key cryptosystem such as RSA[8].

6. LITERATURE REVIEW

Ashish Sharma, Dinesh Bhuriya, Upendra Singh, Secure Data Transmission on MANET by Hybrid Cryptography Technique, IEEE[1], 2015, In this paper they have focused only active attacks in network layer. Ad Hoc On-Demand Vector Routing protocol is a reactive routing protocol for ad hoc networks that maintains route only between nodes those wants to communicate by using routing messages. AODV provide loop free routes during link breakages. SAODV is a secure routing protocol based on trust model for mobile ad-hoc network. To provide security and increase performance in MANET, They have applied SAODV protocol and their solution uses Hybrid Cryptography Technique (DES, RSA Algorithms) on SAODV.

Raj Kamal Kapur, Sunil Kumar Khatri, Secure Data Transfer in MANET Using Symmetric and Asymmetric Cryptography, IEEE[2], 2015,In this paper they have proposed a technique which provides secure transmission of data. The technique involves encryption of data using symmetric cryptographic technique, and also generating the digital signature of the data using the asymmetric cryptographic technique from the Hash of the data. The encrypted data is transmitted through the network to the destination where the received data and digital signature of the data are validated using symmetric and asymmetric cryptography. The data on validation is accepted thus ensuring secure data transmission. The proposed technique provides confidentiality, integrity, authenticity and non-repudiation to the data. It protects the data transmitted over the network from snooping, modification, replay and fabrication attack at the application layer.

Utpal Kumar Verma, Sushil Kumar, Ditipriya Sinha, A Secure and Efficient Certificate based Authentication Protocol for Manet, IEEE[3], 2016, this paper presents a robust and secure mechanism for authentication of nodes in the MANET. The proposed authentication protocol is based on certificate exchange between the nodes. This protocol also uses digital signature with a hash function to maintain the authenticity of certificates. Simulation shows that this protocol shows better performance in terms of throughput, end-to-end delay and packet dropping in presence of malicious nodes in the MANET.

Shreyas S. Jathe, Vidya Dhamdhere, Hybrid Cryptography for Malicious Behavior Detection and Prevention System for MANETs, IEEE[4], 2015, In this paper, They have proposed a system, which can provide high security when information is sent from one place to another place. The system is called as Hybrid Cryptography. Hybrid Cryptography gives a better security than the traditional approaches. In existing system less security provider is used. In this paper, to reduce network overhead, packet delivery ratio caused by existing system, they are using the concept of (RSA) Rivest, Shamir Adleman and (DES) Data Encryption standard algorithm along with the digital signature.

Ms.Trupti Patil, Dr.Bharti Jos, Improved Acknowledgement Intrusion Detection System in MANETs Using Hybrid Cryptographic Technique, IEEE[5], 2015, In this paper MANET has the dynamic topology and it does not have the fixed network infrastructure. Each node acts as the transmitter along with the router. The nodes can communicate with each other either directly or with the help of neighbors. MANET is easily vulnerable to attack due to the open access medium. In this paper they introduce a hybrid technique to reduce network overhead, which is caused by the digital signature and provides security to a network. Here hybrid technique of RSA and AES is used, to make the system more secure.

Ajay Kushwaha, Hari Ram Sharma, Asha Ambhaikar, A Novel Selective Encryption Method for Securing Text over Mobile Ad hoc Network, ELSEVIER[6], 2016, this paper introduces a selective encryption method named Selective significant data encryption (SSDE) for text data encryption. The SSDE provides sufficient uncertainty to the data encryption process as it selects only significant data out of the whole message. This in turn reduces the encryption time overhead and enhances the performance. The encryption part is performed by the help of symmetric key algorithm. For this purpose BLOWFISH algorithm is used.

M.Vijay, R.Sujatha, Intrusion Detection System To Detect Malicious Mis behaviour Nodes in Manet, IEEE[7], 2014, In this paper Mobile Ad Hoc Network (Manet) is one of the most important and unique applications. In this paper Manet infrastructure does not need a fixed network. Every node acts as a transmitter and receiver. Communication occurs within their same communication range only, and communicates directly with each other. Otherwise, they should relay on their neighbors to send relay messages. In open medium and wide distribution of nodes, make Manet vulnerable to malicious attacks. A new instruction detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for Manets. In existing system RSA and digital signature are used. In this paper to reduce the network overhead caused by digital signature by using AES public key cryptography system and AODV routing protocol. To develop efficient instruction detection mechanisms, protect Manet from attacks.

Sivaranjani S, Rajashree S, Secure Data Transfer in Manet Using Hybrid Cryptosystem, IEEE[8], 2014, In this paper various schemes are available for Intrusion Detection systems in Mobile Ad hoc networks (MANET). MANET does not require a fixed network infrastructure; every node works as both a sender and receiver. The security solutions for wireless networks are to provide security services, such as authentication, confidentiality, integrity. The IDS (Intrusion Detection System) is suitable for networks, which detects node misbehavior, anomalies in packet forwarding, such as intermediate nodes dropping or delaying packets is Enhanced Adaptive Acknowledgment (EAACK).

7. CONCLUSION AND FUTURE WORK

In this paper, according to literature review paper study of different security issues, attacks on physical, data and network layers is discussed and also provide security solutions. Various routing protocols discussed in the paper are very helpful and effective for new researchers to identify current issues for advance research. Many new methods, algorithms , protocols are proposed nowadays but still there is an open research issue like which protocol, methods, algorithm shows best behavior in which situation. A lot of contribution has been made in this field but several open problems and issues need to be addressed.

Mobile ad hoc networking is one of the most important and essential technologies that support future computing scheme. Nowadays, MANET is becoming an interesting research topic and there are many research projects employed by academic and companies all over the world.

8. ACKNOWLEDGMENT

We are very much thankful to the IJCA journal for giving us a chance to write paper on our area of interest. We have referred various books and online papers to get the technical knowledge about the mobile ad-hoc networks.

9. REFERENCES

[1] Ashish Sharma, Dinesh Bhuriya, Upendra Singh, Secure Data Transmission on MANET by Hybrid Cryptography Technique, IEEE , 2015.

[2] Raj Kamal Kapur, Sunil Kumar Khatri, Secure Data Transfer in MANET Using Symmetric and Asymmetric Cryptography, IEEE, 2015.

[3] Utpal Kumar Verma, Sushil Kumar, Ditipriya Sinha, A Secure and Efficient Certificate based Authentication Protocol for Manet, IEEE, 2016.

[4] Shreyas S. Jathe, Vidya Dhamdhere, Hybrid Cryptography for Malicious Behavior Detection and Prevention System for MANETs, IEEE, 2015.

[5] Ms.Trupti Patil, Dr.Bharti Jos, Improved Acknowledgement Intrusion Detection System in MANETs Using Hybrid Cryptographic Technique, IEEE, 2015.

[6] Ajay Kushwaha, Hari Ram Sharma, Asha Ambhaikar, A Novel Selective Encryption Method for Securing Text over Mobile Ad hoc Network, ELSEVIER, 2016.

[7] M.Vijay, R.Sujatha, Intrusion Detection System to Detect Malicious Misbehaviour Nodes In Manet, IEEE, 2014.

[8] Sivaranjani S, Rajashree S, Secure Data Transfer In Manet Using Hybrid Cryptosystem, IEEE, 2014.

[9] Muhammad Kashif Nazir, Rameez U. Rehman, Atif Nazir, A Novel Review on Security and Routing Protocols in MANET,SCIRP,2016.

[10] Jagtar Singh, Natasha Dhiman, A Review Paper on Introduction to Mobile Ad Hoc Networks, IJLTET, 2013.