INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Securing MANET Using Diffie Hellman Digital Signature Scheme

Karamvir Singh[1], Harmanjot Singh[2]

[1]Research Scholar, ECE Department, Punjabi University,
Patiala, Punjab, India
[1]*Karanvirk09@gmail.com*

[2]Assistant Professor, ECE Department, Punjabi University,
Patiala, Punjab, India
[2]*Harman.dhaliwal.nba@gmail.com*

Abstract: *A mobile ad hoc network (MANET) is a temporary network formed by the collection of mobile nodes. The network formed does not require any physical infrastructure. There is no central authority to control the services and configurations of the network. How to secure a MANET is an active field of study for researchers. In this paper, we propose the use of security mechanisms for MANETs that are designed based on the characteristics, features, and goals of such networks. We aim to start a paradigm shift in securing MANETs, in which the main focus would be on building security solutions specifically developed for MANETs, and not on adapting solutions that were meant for conventional wired networks. We study the basics and try to propose a simple encryption keys creation scheme that is based on the Diffie Hellman Digital Signature Algorithm. The work presented in this paper would present the initiation of a research agenda designed to build security primitives that are specifically for MANETs, along the lines of the new paradigm.*

Keywords: *Diffie Hellman Digital Signature Scheme, MANET, Security Man-in-Middle attack, Packet Delivery Ratio.*

1. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) are future wireless networks consisting entirely of mobile nodes that communicate on-the-move without base stations. Nodes in these networks would both generate user and application traffic and carry out network control and routing protocols. Rapid changing types of connectivity, network divisions, maximum error rates, collision interference, and increasing bandwidth and power constraints together pose new problems in network control—particularly in the design of higher level protocols such as routing and in implementing applications with Quality of Service requirements .

In a MANET, there is no central entity with the authority to administer the services and configurations of the network. All the nodes work collectively and cooperatively, in a distributed manner, to maintain the functions and services of the network. The distribution of responsibilities and tasks that are meant to keep the network running makes the network resilient to node failures. Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment [1]. Predistribution of cryptographic keys is a widely used approach for establishing secure communication between severely resource-constrained nodes with limited or no access to network infrastructure [7].

2. RELATED WORK

Diffie-Hellman Key Agreement: It was the first practical key distribution and creation protocol that permitted two communicating entities to create a shared key by exchanging information through an open channel, without requiring any prior knowledge to be shared among them [2]. The security of this protocol is based on the computational hardness of the Diffie-Hellman problem and its related problem of calculating discreet logarithms.

2.1 Assumptions

G is a finite cyclic group with a generator g. A and B are two entities who want to establish a shared secret key.

Steps: -

1) A chooses a large random number x such that $0<x<p-1$ and calculate $R_1=g^x \bmod p$

2) B chooses a large random number y such that $0<y<p-1$ and calculate $R_2= g^y \bmod p$

3) A sends R_1 to B ,.

4) B sends R_2 to A

5) A calculates $K=(R_2)^x \bmod p$.

6) B calculates $K=(R_1)^y \bmod p$.

7) Values of keys should be same.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

3. PROBLEMS IN PRESENT WORK

The Diffie-Hellman key exchange is susceptible to two attacks:-

Discrete Logarithm Attack: - The security of key exchange is based on the difficulty of the logarithm problem .Third person can intercept R_1 and R_2. If third person can find x from $R_1 = g^x \bmod p$ and y from $R_2 = g^y \bmod p$ then he can calculate the symmetric key $K = g^{xy} \bmod p$. Thus secret key is not anymore secret.[3-4]

Man-in-middle Attack:- The attacker between A and B do not need to find the values of x and y to attack . He can easily fool A and B by creating two keys: one between himself and A, and another between himself and B. In this way this attack can be successful. B is fooled into believing that the message has come from A and similar scenario can happen to A in other direction. [3] [4] [5]

4. DRAWBACKS OF MOBILE AD-HOC NETWORK

Dynamic topologies: Nodes are easily free to move arbitrarily; thus, the network topology which is typically multi-hop - may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

Bandwidth-constrained, variable capacity links: - Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the measure throughput of wireless communications - after accounting for the effects of multi type of access, fading, noise, and interference situations etc, is often much less than a radio's maximum transmission rate. One effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception, i.e. aggregate application demand would like to approach or exceed network capacity fast [4]. As the mobile network is often simply an extension of the fixed network infrastructure, mobile ad hoc users would demand similar services. These demands would continue to increase as multimedia computing and collaborative networking applications rise.

Energy-constrained operation: Some or rest all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation. So these are the main drawbacks of mobile Ad Hoc network.

5. SECURITY REQUIREMENTS IN MANET

Security and quality of service (QoS) are two areas of mobile ad hoc network (MANET) research which have so far been largely carried out separately [6].Security is the combination of processes, procedures and systems used to ensure confidentiality, authentication, integrity, availability, access control, and non-repudiation.

Confidentiality represents the capability to prevent access to information by unauthorized users or nodes.

Authentication is the ability of an unambiguous confirmation of node identity and simultaneously the ability to prevent taking false identity, a frequent case in wireless networks.

Integrity represents the ability to prevent an unauthorized change or destruction of messages being transmitted within MANET, as well as prevent subsequent messages from the attacker after the unauthorized change.

Non-repudiation is the inability of any node within a MANET to negate the fact that it is a sender of a message [8][9][10]. This requirement is provided by producing a signature for every message

Availability represents the availability of all network services and resources to legitimate network users, which is essential for preserving the network structure during the attacks.

Authorization:- system determines what level of access a particular authenticated user should have to secured resources controlled by the system

6. OBJECTIVES OF THE PROPOSED WORK

Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. A lot of research has been done in the past but the most significant contributions have been the PGP (Pretty Good Privacy) and trust based security. The unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium and highly dynamic network topology. These challenges clearly make a case for building multi-fence security solutions that achieve broad protection. The complete security solution should span both layers, and encompass all three security components of prevention, detection, and reaction.

Following are the major objectives of the proposed work:-

- To reduce the complexity of algorithm to be used for encryption and decryption.
- To reduce the computation at mobile nodes so as to maximize battery life
- To Improve the Overall Performance of the Network.
- To minimize the packet loss ratio in a mobile environment.
- To detect and avoid malicious nodes in the network.

6.1 Description in steps

Step:-1 Network Creation:- Define Network parameters such as number of nodes, Protocol, Channel type etc.

Step:-2 Source and Destination Selection:- After selecting the source and the destination , nodes within the defined range will join together to form a network and start exchanging routing information with each other

Step:-3 Path Selection and Route Computation: - Path will be computed from source to destination on the basis of Hop

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

count. Path computed must have minimum hop count and nodes should have required battery power.

Step:-4 Implementing Man in Middle attack in Mobile ad-hoc Network.

Step:-5 Detecting and removing Man in Middle attack using Diffie Hellman Digital Signature Algorithm. Algorithm used not only provides data integrity but user authentication also.

Suppose ARNOLD = A and BOBY = B

1) After calculating R1, A sends R1 to B.

2) After calculating R2, and session key, B concatenates A's ID, R1 and R2. He then signs the result with his private key. B now sends R2, the signature and his own public key certificate to A. The signature is encrypted with the session key.

3) After calculating the session key, if B's Signature is verified, A concatenates B's ID, R1 and R2. He then signs the result with his own private key and sends it to B. The signature is encrypted with session key.

4) If A's Signature is verified, B keeps the session key

Figure 1 below shows the step by step procedure to implement Diffie Hellman Digital Signature in Mobile Ad-hoc Network.

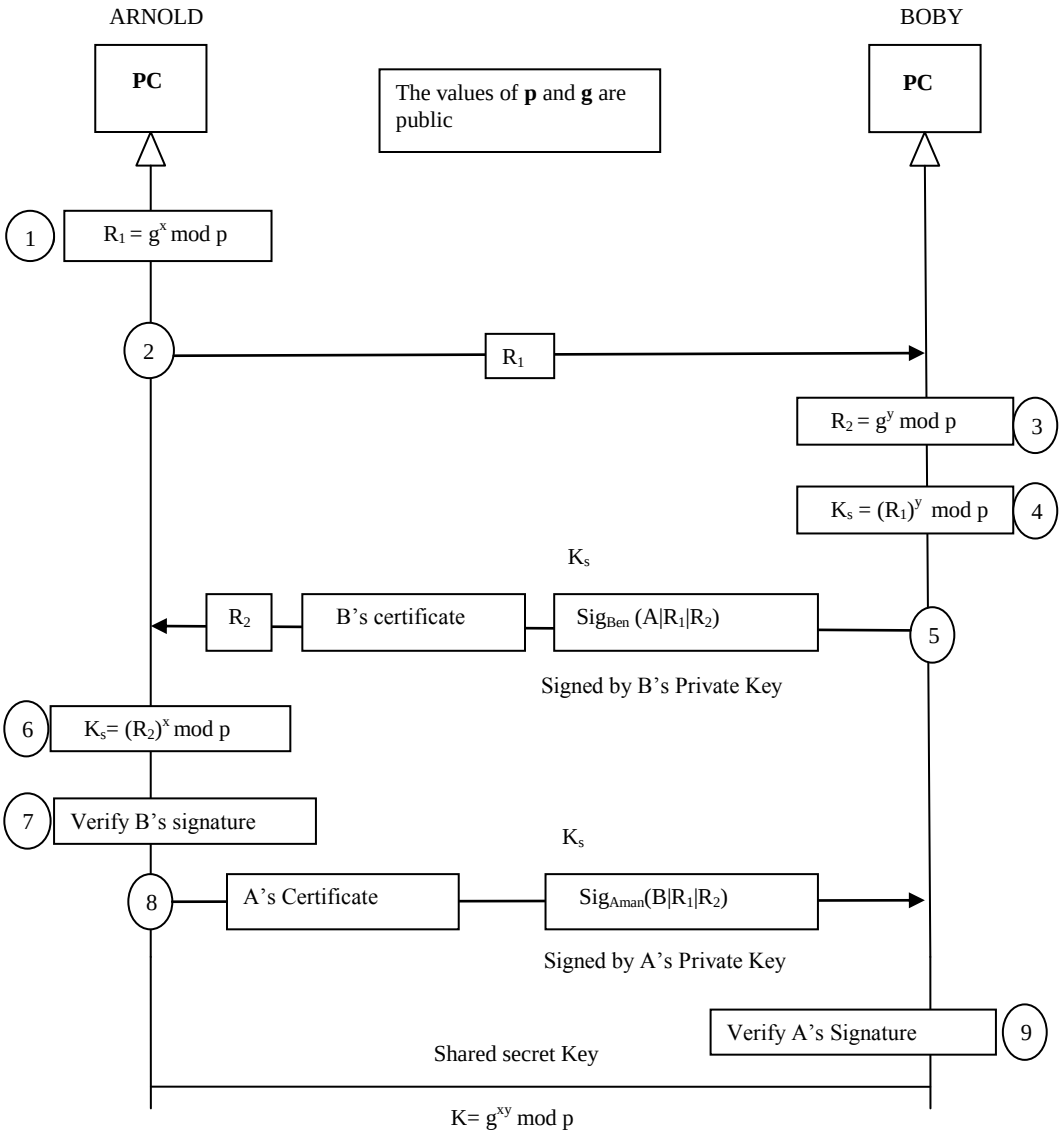

Figure 1: Diffie Hellman Digital Signature Algorithm

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

7. RESULTS AND EVALUATION OF PROPOSED WORK

The Diffie Hellman Digital Signature agreement is preventing Man-in-Middle attack. After intercepting R_1, attacker cannot send his own R_2 value to A and pretend it is coming from B because attacker cannot forget the private key of B to create the Signature – the signature cannot be verified with B's public key defined in the certificate. In the same way, attacker cannot forge A's private key to sign the third message sent by A.

The tool required for implementation is Network Simulator 2(Version 2.35). Ubuntu 13.10 is required for meeting all the conditions of research work. Packet delivery ratio has been calculated under Man in middle attack and without Man in middle attack. Table 1 below shows the number of packets delivered at destination end with or without Man in Middle attack.

Table 1: Packet Delivery Ratio

Time	PDR Under attack	PDR without attack
25	0.9972	0
50	0.9972	0.9684
75	0.9972	0.9901
100	0.9972	0.9943

Figure 2 below shows the graph obtained after implementing Man in Middle attack. Time is along x-axis and Packet Delivery ratio is along y-axis.

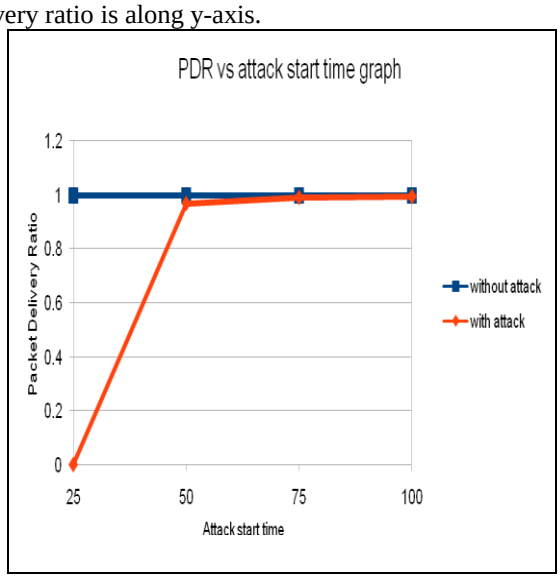

Figure 2: Graph for Packet Delivery Ratio

8. CONCLUSION AND FUTURE DIRECTIONS

In this paper we have Implemented Diffie Hellman algorithm with digital signature to deal with man-in-middle attack. We can use digital signature with other security algorithms for secure communication in MANET. The Mobile ad-hoc network is open to everyone so security is one of the important concerns in MANET. We can also reduce the complexity of algorithm by using digital signature with other security algorithms. Also, the packets sent through the network are safe from Man-in-middle attack as we have used authentication algorithm. Those who want to communicate, has to authenticate themselves first and then they can communicate or exchange information with each other.

For future work, various other methods can be used to encrypt the message after generating the session key. Security can be improved further but keeping the computation overheads normal. A new parameter can be defined for path computation in MANETs whose performance will be better than the earlier ones.

REFERENCES

[1]. **H. Yang, H. Luo, F. Ye, S. Lu and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Communications, doi: 10.1109/ MWC.2004. 1269716**

[2]. **Abdul rahman H. Altalhi , "A Simple Encryption Keys Creation Scheme in Wireless Ad Hoc Networks" , Scientific Research Publishing.**

[3]. **G.S. Mamatha, Dr. S.C. Sharma, "Network Layer Attacks and Defense Mechanisms in MANETS- A Survey", International Journal of Computer Applications.**

[4]. **Sunil Taneja and Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks" , International Journal of Innovation, Management and technology.**

[5]. **PRADIP M. JAWANDHIYA, "A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology http://www.ijest.info/docs/IJEST10-02-09-22.pdf**

[6]. **Peter J. J. McNerney and Ning Zhang, "Towards an Integration of Security and Quality of Service in IP-Based Mobile Ad Hoc Networks" , IEEE Globecom 2011.**

[7] **R. Novales and N. Mittal, "Parameterized Key Assignment for Confidential Communication in Wireless Networks," *Ad Hoc Networks*, Vol. 9, No. 7, 2011, pp. 1186-1201. Doi: 10.1016/ j.adhoc. 2011.01.009**

[8]. **J. Lee and D. R. Stinson, "On the Construction of Practical Key Pre-distribution Schemes for Distributed Sensor Networks Using Combinatorial Designs," *ACM Trans- actions on Information and System Security* (*TISSEC*), Vol. 11, No. 2, 2008, pp. 1-35. doi:10.1145/1330332.1330333**

[9]. **S. Capkun, J. Hubaux and L. Buttyan, "Mobility Helps Peer-to-Peer Security," *IEEE Transactions on Mobile Computing*, Vol. 5, No. 1, 2006, pp. 43-51. doi:10.1109/TMC.2006.12**

[10]. **E. Bresson, O. Chevassut and D. Pointcheval, "The Group Diffie-Hellman Problems," In: K. Nyberg and H. Heys, Eds., 9*th* *Annual International Workshop on Se-lected Areas in Cryptography* (*SAC*'02), Springer-Verlag, London, 2002, pp. 325-338.**