# Improving Security & QoS in IP-Based MANETs

Talwinder Singh , Anurag Singh Tomar

***Abstract*-**A mobile ad hoc network (MANET) is a temporary network formed by the collection of mobile nodes. The network formed do not require any physical infrastructure. There is no central authority to administer the services and configurations of the network. Securing MANETs is still an active area of research. In this paper, we propose the use of security mechanisms to improve the security as well as QoS in MANET. A combination of different parameters will be considered to compute optimal path from source to destination and use a simple key agreement scheme that is based on the Station-to-Station key agreement protocol.

***Index Terms*:-** Energy level , Hop count , Key Management, MANET Security, QoS, Symmetric Encryption Keys , Station-to-Station Key agreement

## 1. INTRODUCTION

The spontaneous growth of technology for mobile devices, including laptops and computers, and the availability of cheap wireless networking [1] hardware, has resulted in a great demand for wireless connectivity among mobile users. One approach to providing wireless connectivity is through the formation of a mobile ad hoc network .

A mobile ad hoc network (MANET) [1] is a collection of mobile nodes that temporarily integrate to form a network. Such type of network does not require the use of the typical infrastructure underlying a network. Rather, each mobile node is equipped with a wireless interface that allows the node to communicate with other nodes via the wireless medium. Handheld computing devices and laptop computers with wireless transceivers are examples of mobile nodes that can come together to form a MANET. 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. It also allows nodes to join and leave the network liberally with- out affecting the network′s operability.

## 2. LITERATURE SURVEY

Security has become a primary concern in order to provide protected communication between mobile nodes in a dynamic environment. Unlike the wired network, the unique features of mobile ad hoc networks pose a number of nontrivial challenges to security design, like open peer-to-peer network architecture, shared wireless medium, resource constraints, and dynamic network structure. These characteristics clearly make a case for building multi-fence security solutions that can achieve broad protection with desirable network performance.

### 2.1 Session key generation Algorithm

Diffie-Hellman Key Agreement :- It was the first practical key distribution [1] 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 . This solution is a perfect match for the issues involved in forming a MANET. The security of this protocol is based on the computational hardness of the Diffie-Hellman problem and its related problem of calculating discreet logarithms .The Diffie-Hellman protocol works as follows

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.

### 2.2 Weakness in Deffie Hellman Algorithm

The Deffie-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.

Man-in-middle Attack:- The attacker between A and B do not need to find the values of x and y to attack . He

IJSER © 2013
http://www.ijser.org

can easily fool A and B by creating two keys : one be 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. ISSUES AND DIFFICULTIES IN MANETS

MANET is different from the conventional wired networks. This difference introduced few difficulties in achieving Quality of Service in such networks. The following are the problems :-

Dynamic Network topologies**:-** Nodes can move freely, thus, the network topology[3] 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 then wired one. In turn, the measured throughput of wireless communications - after accounting for the effects of multiple access, fading, noise, deterioration and interference conditions ,etc.- is often much less than a radio's maximum transmission rate. So, effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception, i.e. total application demand will likely approach or exceed network capacity frequently . As the mobile network is often simply an advancement of the fixed network infrastructure, mobile ad hoc users will demand same services.

Energy-constrained operation**:-** Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the important system design scheme for optimization may be energy conservation.

## 4. OUR PROPOSED MACHNISMS FOR SECURITY AND QoS:-

**STEP :- 1** Creation of network :-

There are number of mobile nodes roaming freely and independently. A specific range will be defined for the node to be the part of the network . if the node comes in the defined range then it will join the network.

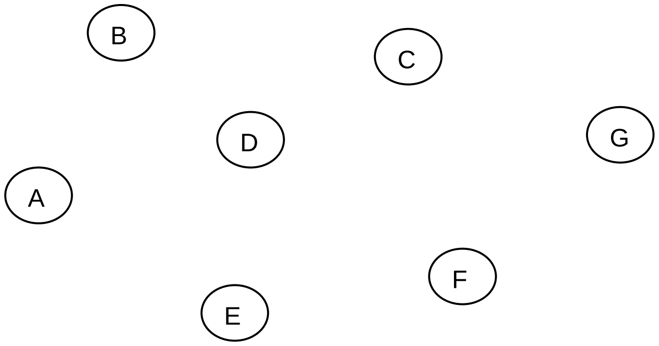

Fig :- 1 Mobile Nodes

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

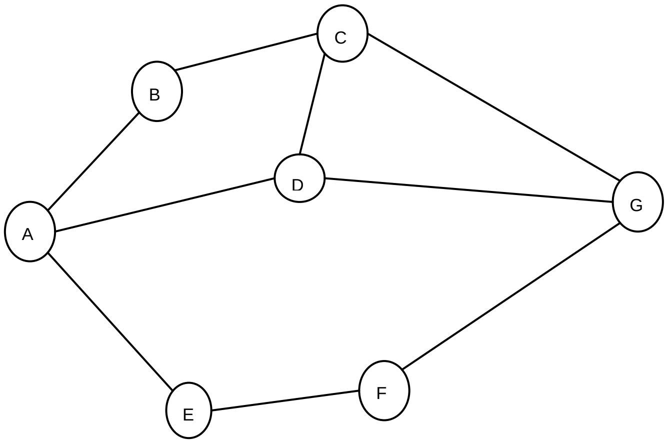

Fig:-2 Mobile nodes creating a network

**STEP:- 3** Path Selection and Route Computation

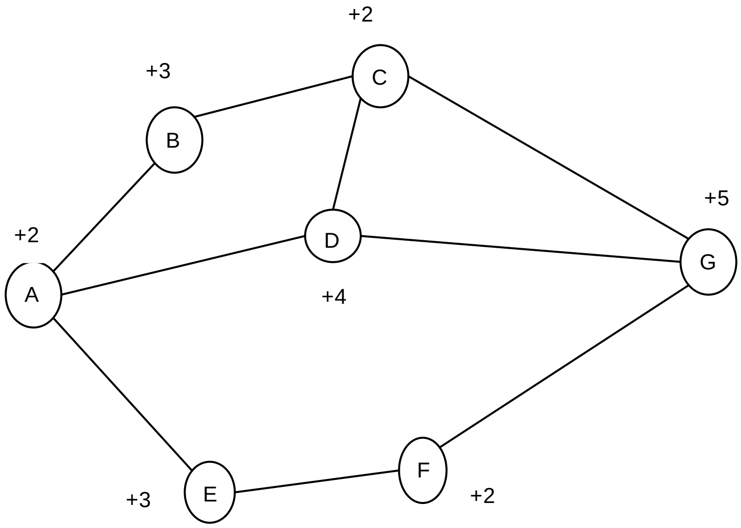

Fig :-3 Mobile ad-hoc network with energy levels

Table :- 1

| Source | Destination | Possible Path | Hop Count | Energy level |
|---|---|---|---|---|
| A | G | A-B-C-G<br>A-D-C-G<br>A-B-C-D-G<br>A-D-G<br>A-E-F-G | 3<br>3<br>4<br>2<br>3 | 12<br>13<br>16<br>11<br>12 |

In the given diagram we have source node A and Destination node G. Hope count and Energy level are the only two parameters considered in this scenario . We have different paths from source to destination:-

A-B-C-G
A-D-C-G
A-B-C-D-G
A-D-G [Least Hop count]
A-E-F-G

First of all we will choose path with least hop count and check if there is any node in this path with 0 and +1 energy level. if node with 0 and +1 energy level exist then we will simply skip this path and select the 2nd path with least hop count. Repeat the same process and send the data through the best selected path.

Path Selected: - A-D-G

While sending data from source to destination various parameters are considered to compute path , for example :- hop count , energy level , trust level etc.

In our proposed solution, we will calculate path from source to destination by using two factors together, i.e hop count and energy level.

Hop count will calculate the shortest path while energy level will help us in calculating the path through those nodes which has high energy level. In this way the optimum path will be considered for sending data. Moreover , it will eliminate the problem of data loss due to link breakage in MANETs.

**STEP: - 4** Condition when a Node goes out of range

In the given diagram node L is going out of range and it will leave the network. Now, nodes will again exchange information with each other and update their tables accordingly.

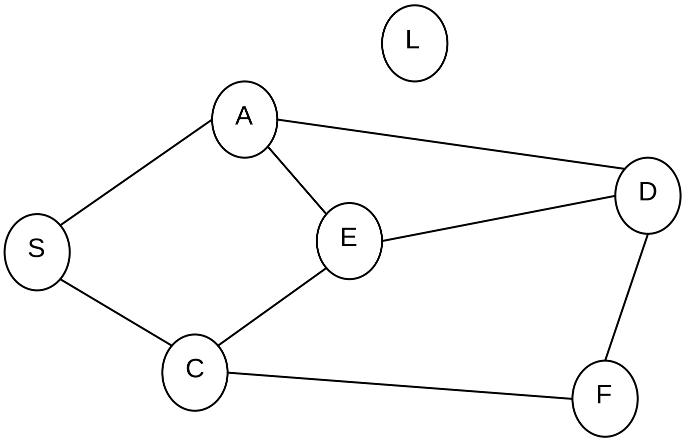

Fig :- 4 Mobile node going out of range

**STEP :- 5** Condition when a new node join the network

When a new node join the network , again all the nodes in the network will exchange information with each other and update their tables accordingly

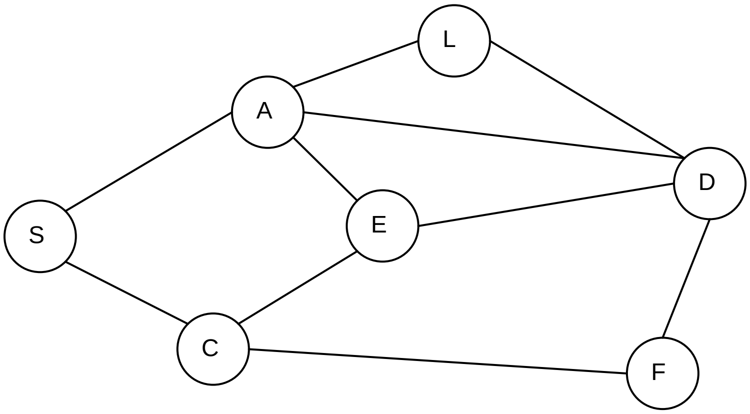

Fig :-5 New node joining the network

IJSER © 2013
http://www.ijser.org

**STEP :- 6** Session key generation algorithm

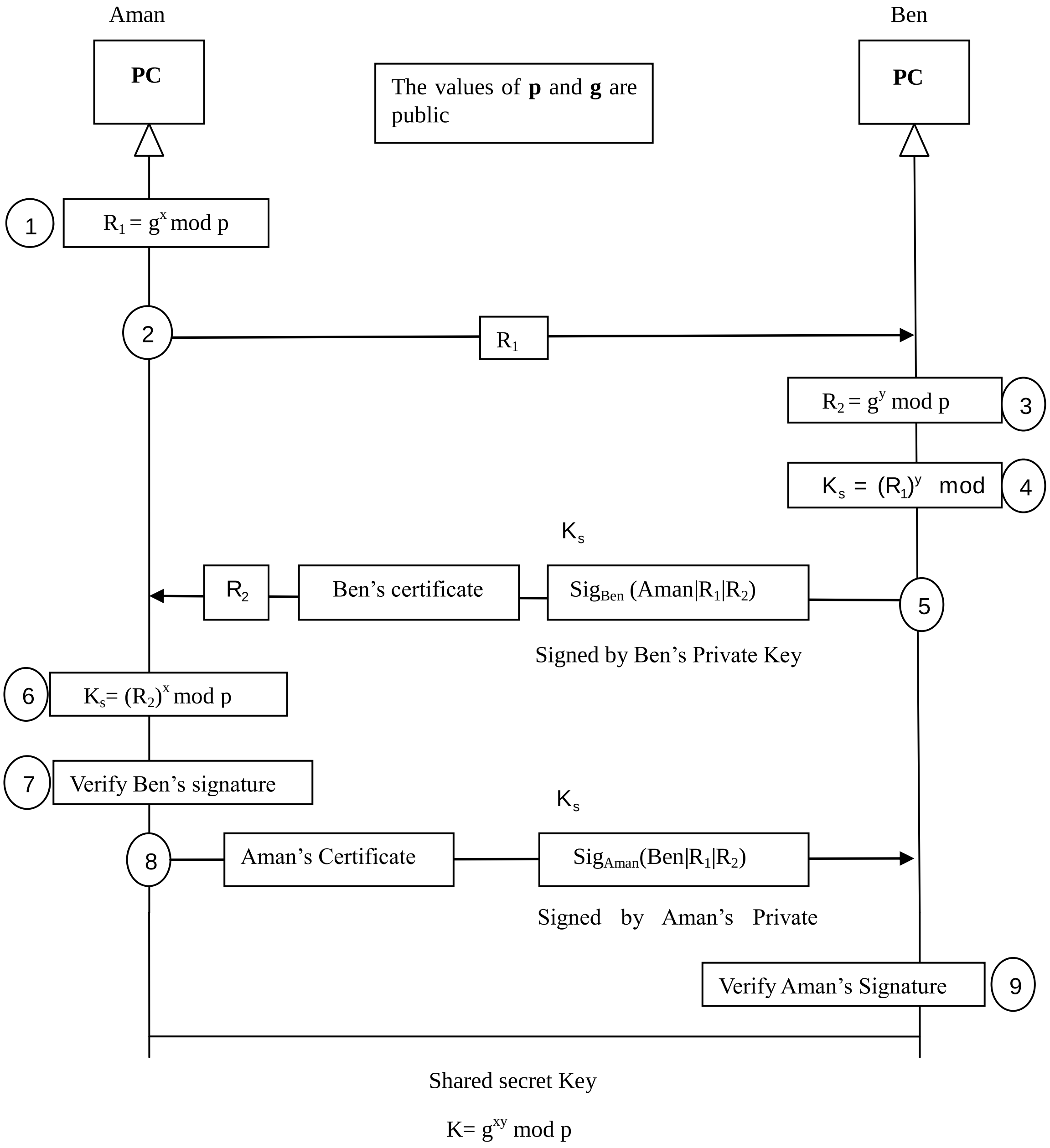

Fig :- 6 Station-to-Station key agreement in MANETs

In our proposed mechanism we are using Station-to-Station key agreement [14] to deal with the problems in Deffie Hellman key agreement. This method use digital signature with public-key certificates to establish a session key between A and B. This method provides integrity as well as authentication .

We have implemented station-to-station key agreement in MANETs for generating session key and thus provide secure communication. After generating secret key we can encrypt the text using any of the encryption algorithm without affecting the overall QoS.

Description in steps

Suppose Aman = A and Ben = B

1) After calculating $R_1$, A sends $R_1$ to B.
2) After calculating $R_2$, and session key , B concatenates A's ID , $R_1$ and $R_2$. He then signs the result with his private key. B now sends $R_2$, 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 , $R_1$ and $R_2$ . 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

Key agreement will be between source and destination only (end to end) and to avoid computation overheads only the payload portion will be encrypted.

## 5. STRENTH OF PROPOSED SOLUTIONS:-

The Station-to-Station key agreement prevents man-in-middle attacks . After intercepting $R_1$, attacker cannot send his own $R_2$ value to A and pretend it is coming from B because attacker cannot forge 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.

Link breakage is one of the major problem in MANETs because of the mobility of nodes or power available in each node. In our proposed solution we have removed the problem of link breakage by considering energy level of every node in the ad-hoc network.

## 6. CONCLUSIONS

In this paper we created session key using Station-to-station key agreement. This key will be used in MANETs for secure communication. The Mobile ad-hoc network is open to everyone so security is one of the important concern in MANETs. 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.

There many other parameters such as trust level , bandwidth , route repetition etc . These parameters can also be combined to improve the overall QoS in MANETs.

## 7. Acknowledgements

My sincere thanks to my honourable guide and others who have contributed towards the preparation of the paper.

## 8. REFRENCES

[1]. Abdulrahman H. Altalhi , "A Simple Encryption Keys Creation Scheme in Wireless Ad Hoc Networks" , Scientific Research Publishing www.scirp.org/ journal/ PaperDownload.aspx?DOI=10.4236/ cn

[2]. 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 http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6133684&contentType=Conference+Publications

[3] Jianbo Xue , Dr. Gustavo Alonso , "Quality of Service for Mobile Ad Hoc Networks" , ETH SFT 2003 http:/ / ijarcsee.org ›/ Home/ Vol 1, No 7 (2012) / Panda

[4]. 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

[5] G.S. Mamatha , Dr. S.C. Sharma , "Network Layer Attacks and Defense Mechanisms in MANETS- A Survey" , International Journal of Computer Applications www.ijcaonline.org/volume9/number9/pxc3871911.pdf.

[6] Sunil Taneja and Ashwani Kush , "A Survey of Routing Protocols in Mobile Ad Hoc Networks" , International Journal of Innovation, Management and technology http:/ / www.minema.di.fc.ul.pt/report_routing-protocols-survey-final.pdf

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

[8] 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

[9] J. Lee and D. R. Stinson, "On the Construction of Pra- ctical Key Predistribution 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

[10] 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

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

[12] E. Ngai, M. Lyu and R. Chin, "An Authentication Service against Dishonest Users in Mobile Ad Hoc Networks," *Proceedings of the* 2004 *IEEE Aerospace Conference*, Big Sky, Vol. 2, 6-13 March 2004, pp. 1275-1285.

[13] S. Zhu, S. Xu, S. Setia and S. Jajodia, "LHAP: A Light-weight Network Access Control Protocol for Ad Hoc Networks," Ad Hoc Networks, Vol. 4, No. 5, 2006, pp. 567-585. doi:10.1016/ j.adhoc.2006

## Books :-

[14] Behrouz A. Forouzan, Debdeep Mukhopadhyay , *cryptography and network security* second edition Mc graw Hill (2010).