Secret Key Establishment for Symmetric Encryption over Adhoc Networks

Sunil Taneja[1], Ashwani Kush[2] and C. Jinshong Hwang[3]

***Abstract*— The adhoc environment is accessible to both legitimate network users and unfortunately to malicious attackers as well. Secure routing over mobile adhoc networks is hard to achieve because of dynamic topology, mobility of nodes, lack of centralized infrastructure and absence of a certification authority. When a new mobile node joins the network and it does not have any trust based relationship with other nodes in the network, the problem of secure routing may arise. While implementing data encryption and decryption in a symmetric cryptosystem, secure distribution of the secret key to legitimate nodes can be a challenge. In this paper, common secret key has been established for symmetric encryption over adhoc networks using Diffie-Hellman key agreement protocol. The concept can be used to develop a new routing protocol for mobile adhoc networks which will provide maximum security against all kinds of attacks.**

***Index Terms*—Adhoc, Encryption, Key, Networks, Private, Protocol, Public, Security**

I. INTRODUCTION

In mobile adhoc networks [3], the nodes can move while communicating, there are no fixed base stations and all the nodes in the network act as routers as well as hosts to facilitate the unconstrained mobility. The mobile nodes in the adhoc network dynamically establish routing among themselves to form their own network 'on the fly'. The special features of adhoc networks bring great technological opportunities together with different challenges. Some of the challenges in the area of adhoc networks include autonomous behaviour, unicast/multicast routing, dynamic network topology, limited resources, network overhead, scalability, stable routing, secure routing and power-aware routing. Our focus in this paper is on the security of wireless adhoc networks. The nodes over adhoc network need to be sure that they are actually communicating with the intended recipient and some other devices are not masquerading as a legitimate one. The dilemma is that how should we judge whether the adhoc network is secure or not. There have been numerous published reports and papers describing attacks on wireless networks [8] that expose organizations to security risks such as attacks on confidentiality, authenticity, availability, integrity, non repudiation and authorization. There are several proposals to solve these issues but they target specific threats separately. Therefore, there is a requirement to have an efficient security system which takes care of all aspects of security.

[1]Department of Computer Science, Smt. Aruna Asaf Ali Government P.G. College, Kalka, Pin Code: 133302, Haryana, India (phone: +919467237272; e-mail: suniltaneja.iitd@gmail.com).

[2]Department of Computer Science, University College, Kurukshetra University, Kurukshetra, Pin Code: 132119, Haryana, India (e-mail: akush20@gmail.com).

[3]Department of Computer Science and Engineering, Texas State University, San Marcos, Texas, USA (e-mail: cjhwang@txstate.edu)

In this paper, secret key establishment for symmetric encryption over adhoc networks using Diffie-Hellman key agreement protocol has been presented. The concept can be used to develop a new secure routing protocol which takes care of maximum security attributes collectively. Rest of the paper is organized as: section II is about recent studies carried out in the field of secure routing over adhoc networks. This section elaborates on secret key establishment for adhoc networks. Section III illustrates Diffie-Hellman key agreement protocol which is composed of four stages. In section IV, working model of this protocol has been demonstrated by taking an example of two of the most widely traveled Internet users in cyberspace i.e. Alice and Bob. Section V elaborates on a case study of this protocol and at last, section VI concludes the paper and provides an idea to researchers about challenges in the field of secure routing over ad hoc networks that may be carried out as research work in future.

II. RECENT STUDY

The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form is known as cryptography [9].

A. Symmetric Encryption

In a symmetric-key algorithm both parties use the same key for encryption and decryption. The plain text message *m* is encrypted using the shared key *k*, resulting in the cipher text *c*. To recover the plain text message the cipher text is decrypted using the same key used to for the encryption.

B. Public Key Encryption

Unlike symmetric encryption whereby the involved parties share a common encryption/decryption key, public key encryption algorithms (asymmetric cryptography algorithms) use two different keys for encryption and decryption which are mathematically interrelated. Here each node in the network has a pair of keys, the private key and the public key.

Chan Chen and Jensen M.A. [2] has worked on secret key establishment using temporally and spatially correlated wireless channel coefficients. The studies assist in the development of a practical key generation protocol based on a published channel coefficient quantization method and incorporating flexible quantization levels, transmission of the correlation eigenvector matrix, and LDPC coding to improve key agreement in an authenticated public channel.
Lehane B et al [6] have carried out research on generation of shared RSA key in a mobile ad hoc network. The use of distributed shared RSA key generation techniques to create a threshold certificate authority 'from scratch' has been described. The goal is to create a scalable key management solution which does not rely on prior infrastructure for its

ISBN: 978-988-19251-7-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

inception and as such is formed in a truly ad hoc manner compatible with the formation of the network itself. S. Sumathy and B. Upendra Kumar [7] proposed a secure key exchange and encryption mechanism for group communication in wireless adhoc networks that aims to use the MAC address as an additional parameter as the message specific key *[to encrypt]* and forward data among the nodes. The proposed scheme consists of RSA key exchange mechanism and a novel encryption mechanism to provide security. Each node in the network has its own symmetric key called the neighborhood key. To perform encryption and decryption each node must have access to other nodes neighborhood key. At source, neighborhood key is encrypted with the public key of the receiver and transmitted to the destination node. At destination, neighborhood key is decrypted with the node's own private key. The nodes are organized in spanning tree fashion, as they avoid forming cycles and exchange of key occurs only with authenticated neighbors in ad hoc networks, where nodes join or leave the network dynamically.

The work carried out by these eminent researchers has been taken into consideration while proposing a new secure routing protocol. Basically, the nodes over adhoc network need to be sure that they are actually communicating with the intended recipient and some other devices are not masquerading as a legitimate one. The dilemma is that how should we judge whether the ad hoc network is secure or not. The main security criteria's that are used to inspect the security state of the adhoc networks are confidentiality, authenticity, integrity, availability, non repudiation and authorization. The main threats that violate these security criteria are known as attacks. These security attacks are typically divided into two categories: passive vs. active attacks. The consequences of these attacks include, but are not limited to, loss of proprietary information, legal and recovery costs, tarnished image, and loss of network service. In this paper, we considered establishing common secret key for symmetric encryption over adhoc networks using Diffie-Hellman key agreement protocol which will provide maximum security against all kinds of attacks.

III. DIFFIE-HELLMAN KEY AGREEMENT PROTOCOL

Establishment of common secret key is very important in wireless adhoc networks. The issue becomes more crucial because of lack of centralized infrastructure in adhoc networks. Diffie-Hellman key agreement protocol uses a symmetric system to encrypt the data and an asymmetric system to encrypt the symmetric keys. Figure 3 illustrate Diffie-Hellman key agreement protocol which is composed of following stages [5]:

A. Key Generation and Exchange
B. Shared Secret Creation
C. Encrypting, Passing, and Decrypting the Symmetric Key
D. Encrypted Data Transmission

A. Key Generation and Exchange

Each side of the communication generates a private key (number 1) and then generates a public key (number 2), which is a derivative of the private key. The two systems then exchange their public keys. Each side of the communication now has their own private key and the other systems public key (number 3). The Diffie-Hellman protocol has a "Certificate Authority" to certify that the public key is indeed coming from the source you think it is. The purpose of this certification is to prevent the 'Man In the Middle' (MIM) attacks.

B. Shared Secret Creation

Once the key exchange is complete, the Diffie-Hellman algorithm generates shared secrets, an identical cryptographic key shared by each side of the communication. The value of key is generated by using a mathematical operation against your own private key and the other side's public key. Figure 3 depicts this operation with the "DH Math" box. When the distant end runs the same mathematical operation against your public key and their own private key, they also generate a value. The important point is that the two values generated are identical.

C. Encrypting, Passing, and Decrypting the Symmetric Key

The shared secret, by its mathematical nature, is an asymmetric key that could encrypt traffic. If the two sides are passing very little traffic, the shared secret may encrypt actual data. Any attempt at bulk traffic encryption requires a symmetric key system such as DES and IDEA etc. In most real applications of the Diffie-Hellman algorithm, the shared secret encrypts a symmetric key, transmits it securely, and the distant end decrypts it with the shared secret. Figure 3 also illustrate this operation. It is most common for the initiator of the communication to be the one that transmits the key.

D. Encrypted Data Transmission

Once secure exchange of the symmetric key is complete, data encryption and secure communication can occur. Figure 1 also depicts data encrypted and decrypted on each end of the communication by the symmetric key.

IV. WORKING MODEL OF DIFFIE-HELLMAN KEY AGREEMENT PROTOCOL

This protocol has been demonstrated by taking an example of two of the most widely traveled Internet users in cyberspace, Alice and Bob. The key concept behind this algorithm is that Alice and Bob agrees upon a shared secret that an eavesdropper will not be able to determine. This shared secret is used by Alice and Bob to independently generate keys for symmetric encryption that will be used to encrypt the data stream between them. The main point is that neither the shared secret nor the encryption key ever travels over the network. For implementation purposes Alice can be treated as Source and Bob as Destination or neighbor node participating in route to Destination. CrypTool [1] has been used as a simulator for the purpose. It is an open-source e-learning application, used in the implementation and analysis of cryptographic algorithms. It provides a fully developed architecture and rich cryptographic functionality combined with a pioneering GUI, featuring a visual presentation of cryptographic protocols. We have focused on the working model of Diffie-Hellman key agreement protocol whereby the separation between Alice and Bob is demonstrated respectively by two different private areas and nobody else except authorized party gains an insight into these private areas.

ISBN: 978-988-19251-7-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

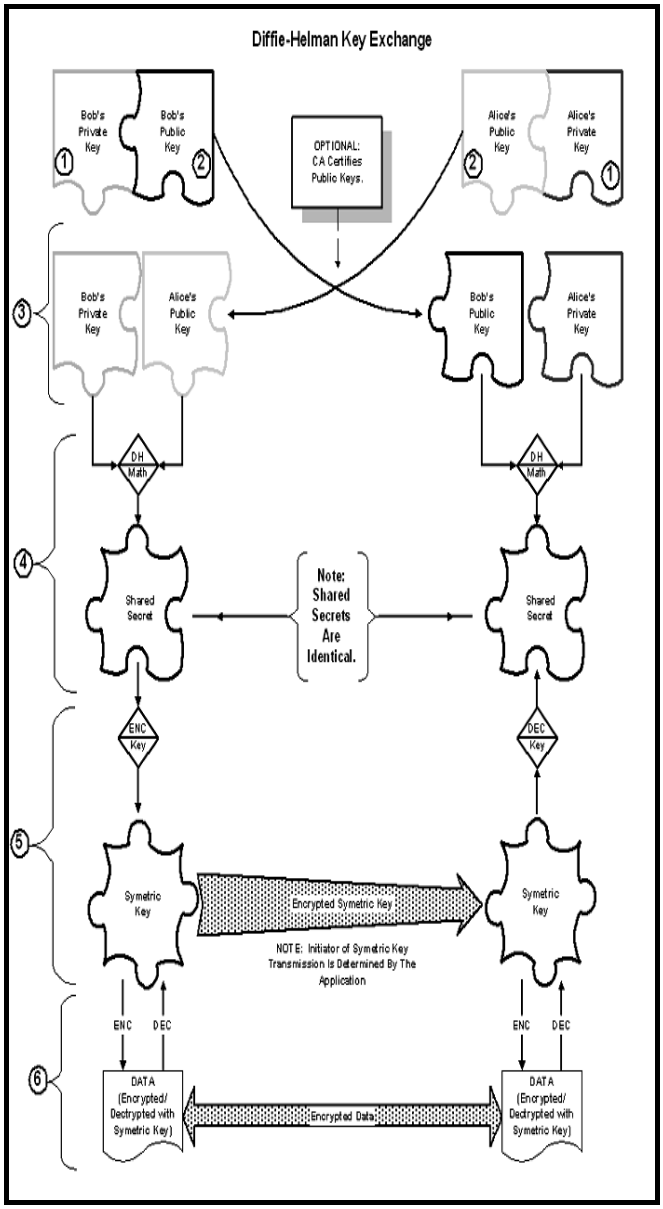

Figure 1: Diffie-Hellman key agreement algorithm [5]

As a first step, public parameters are set. Since the public parameters are freely accessible to all and therefore, not only Alice and Bob are able to access these parameters rather every third party too can observe the same. Figure 2 demonstrate setting of these parameters. Once the public parameters are set, secret numbers of Alice and Bob are chosen by pushing the button choose secrets as shown in figure 3. After this the shared keys of Alice and Bob is created as shown in figure 4 and 5. Now Alice sends her shared key over to Bob and Bob sends his shared key over to Alice. It means shared keys are now exchanged and the same has been shown in figure 6. As a last step, Alice and Bob create common and secret session key by pushing the button generates common session key as shown in figure 7.

Using the secret information on the one end and the public information on the other end, each party, Alice and Bob, computed the common and secret key on its own as shown in figure 8.

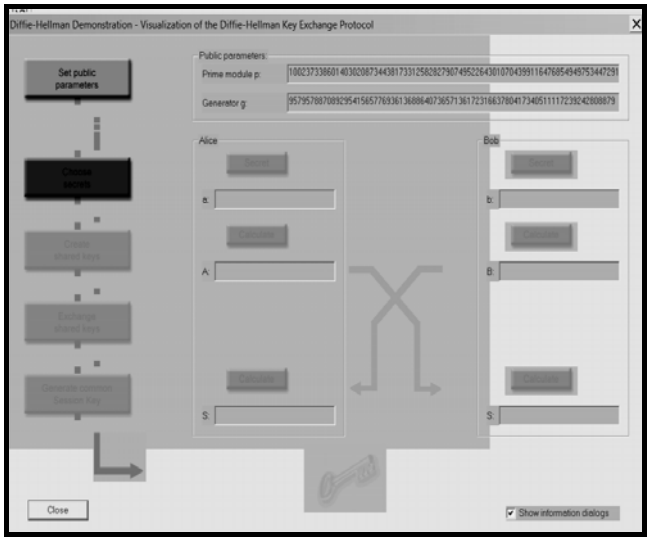

Figure 2: Setting the public parameters

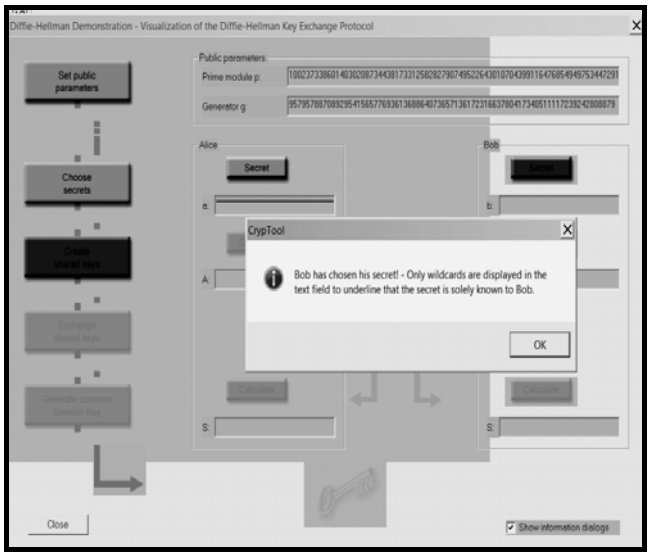

Figure 3: Choosing the Secrets

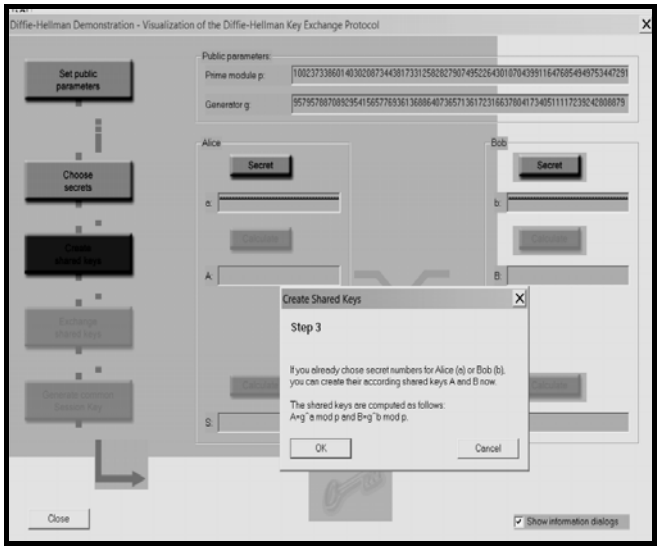

Figure 4: Create shared keys

ISBN: 978-988-19251-7-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

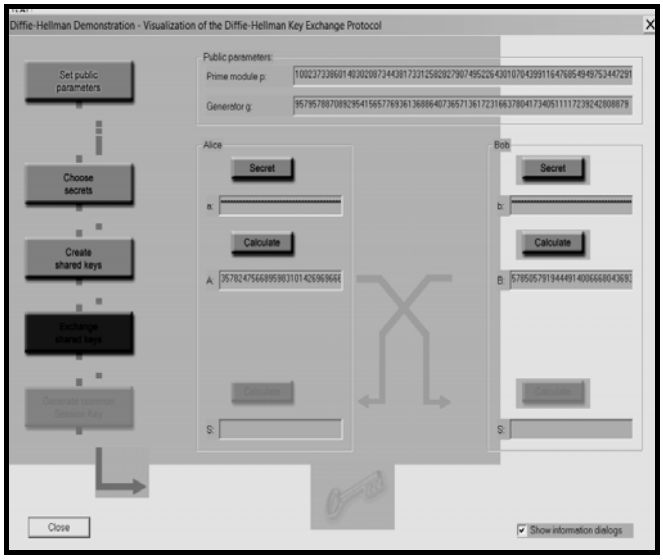

Figure 5: Calculating the shared keys

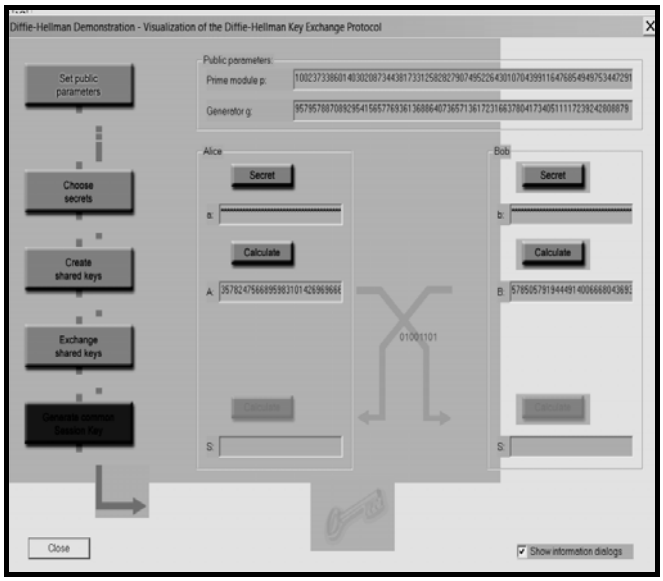

Figure 6: Exchange of shared keys

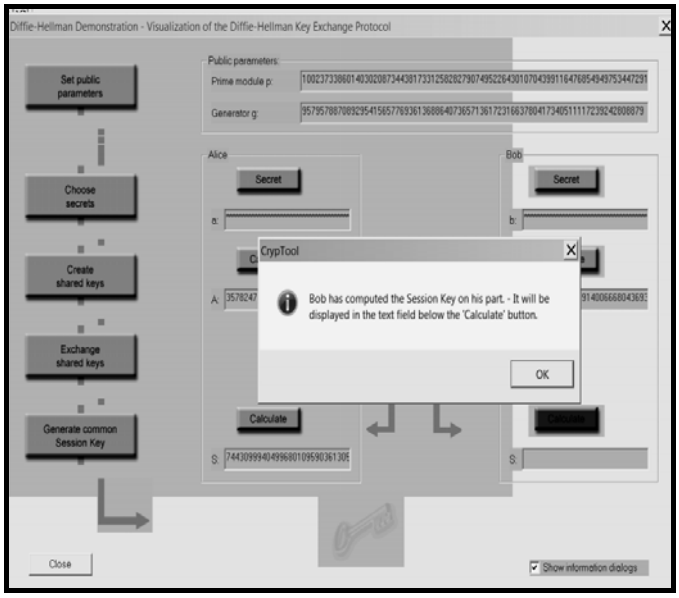

Figure 7: Create common and secret session key

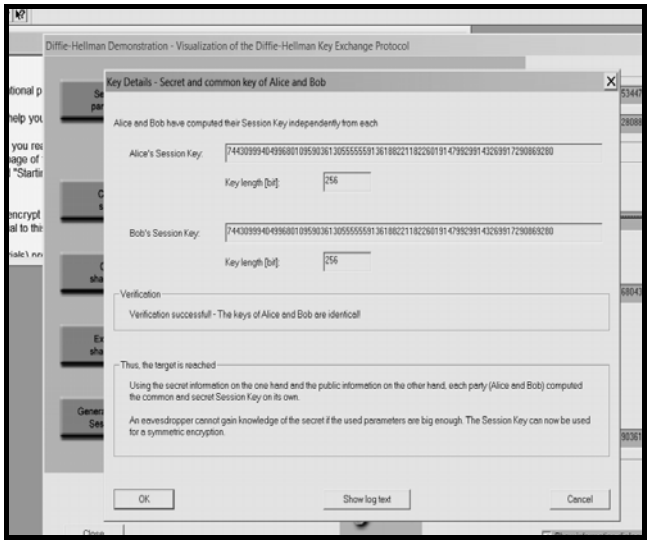

Figure 8: Common and secret session keys

V. CASE STUDY

Alice and Bob agreed on the public parameters ‘p’ and ‘g’. Alice chooses her secret number 'a' while Bob chooses his secret number 'b'. If the chosen secret values a and b are greater or equal the prime module p, then they need to be reduced modulo p. Then on the basis of chosen secret numbers, Alice and Bob created their shared keys A and B. In order to calculate their secret and common session keys, they exchanged their shared keys. Alice sent her shared key A to Bob and Bob sent his shared key B to Alice. As a case study the following example has been used.

p:
100237338601403020873443817331258282790749522643
010704399116476854949753447291
g:
957957887089295415657769361368864073657136172316
637804173405111172392428088 79

a:
744259531694568904235623632373840409376332584777
379627065877833878525125884 74
b:
187754744006544448270606742390374991710730955519
470400188756368354278163389 01

a (reduced mod p):
744259531694568904235623632373840409376332584777
379627065877833878525125884 74
b (reduced mod p):
187754744006544448270606742390374991710730955519
470400188756368354278163389 01

A:
357824756689598310142696966655493255871159419192
361475192482739805707178274 88
B:
578505791944491400666804369355119947126216871062
716270943821269765666931832 54

Session Key A:
744309994049968010959036130555555913618822118226
019147992991432699172908692 80

ISBN: 978-988-19251-7-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Session Key B:
744309994049968010959036130555555913618822118226
019147992991432699172908692 80

An eavesdropper cannot gain the knowledge of the secret if the used parameters are big enough. This secret key can now be used as a session key in order to do symmetric encryption over adhoc networks. This concept can be implemented in AODV protocol so as to develop a new secure on-demand routing protocol. This will ensure secure transmission of data between the entities involved in communication over adhoc networks.

VI. CONCLUSION

Areas have been identified in the field of secure routing where work need to be carried out. The Diffie-Hellman key agreement protocol uses the secret information on the one end and the public information on the other end for communication between source and destination nodes. It is just impossible for eavesdroppers to know the secret key if the used parameters are big enough. This secret key is used as a session key in order to do symmetric encryption. The findings can be used to develop a new secure routing protocol for mobile adhoc networks that takes care of all aspects o security. Efforts are on to develop the new secure routing protocol by taking AODV [4] protocol as the base and then to simulate the same by creating different network scenarios over network simulator. Once the new protocol is implemented, the performance will be analyzed with respect to existing secured routing protocols. The ultimate target is to develop a secure routing protocol which provides maximum protection against all kinds of attacks.

REFERENCES

[1] Bernhard Esslinger, "CrypTool, Version 1.4.10", Deutsche Bank AG, Frankfurt/Main, University of Siegen and Darmstadt, July 2007, www.cryptool.org.

[2] Chan Chen, Jensen M.A., "Secret Key Establishment using Temporally and Spatially Correlated Wireless Channel Coefficients, IEEE Transactions on Mobile Computing, Volume 10, Issue 2, pp. 205-215, 2010.

[3] Charles E. Perkins, "Ad Hoc Networking", Pearson Education, 2008.

[4] Charles E. Perkins, E. B. Royer, S. Das, "Adhoc On-Demand Distance Vector (AODV) Routing", IETF Internet Draft, 2003.

[5] Keith Palmgren, "Diffie-Hellman Key Exchange", February 2005, http://www.securitydocs.com /library/2978.

[6] Lehane B., Doyle L., O'Mahony D, "Shared RSA key generation in a mobile ad hoc network", Military Communications Conference, 2003, IEEE Xplore, Volume 2, pp. 814 – 819, 2003.

[7] S. Sumathy and B.Upendra Kumar, "Secure Key Exchange and Encryption Mechanism for Group Communication in Wireless Adhoc Networks", International Journal on Applications of Graph Theory in Wireless Adhoc Networks and Sensor Networks (Graph-Hoc), Volume 2, No. 1, pp. 9-16, 2010.

[8] T. Karygiannis and L. Owens, "Wireless Network Security", NIST Special Publication, November 2002.

[9] William Stallings, "Cryptography and Network Security: Principles and Practice", 5/E, Prentice Hall, 2010.

ISBN: 978-988-19251-7-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)