ISSN : 2231-0711

Vikas Gupta et al | International Journal of Computer Science Engineering and Technology(IJCSET) | June 2014 | Vol 4, Issue 6,208-213

Enhance the Data Security Using PGP & DES in MANET

[1]Vikas Gupta, [2]Harprabhdeep Singh

[1,2] *Adesh Institute of Engineering & Technology, Faridkot*

Abstract: The goal of security solutions is to provide security services, such as authentication, confidentiality, integrity, and availability to mobile users. In order to enhance the security various algorithms were proposed, such as International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES) & Pretty Good Privacy (PGP) etc. Individually each algorithm has one deficiency or the other. The research work is based on the objectives such as establishing the confidentiality of data to prevent reading of data in plain text except of the intended addressee, guarantying the reliability of the source of information (authenticity), preventing someone masked as the author of a message which was actually created by somebody else (protection of intellectual property), to maintain the integrity of a message such that composed message cannot be changed. To achieve these objectives, both the PGP Encryption scheme and DES Algorithm have been combined to enhance the security. The proposed hybrid system using PGP & DES encryption algorithm improves the security of a network by securing the data and preserving the confidentiality.

Keywords: PGP, DES, Data Security, MANET

1. INTRODUCTION

Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defence mechanism. Hence the proposed research work has been attempted to overcome the vulnerability of MANETs against security attacks.

2. LITERATURE REVIEW

Haas (2003) in the paper "Secure Data Transmission in Mobile Ad Hoc Networks" presented an approach on Secure Message Transmission in Mobile Ad hoc Network. The security of data transmission is achieved without restrictive assumptions on the network nodes' trust and network membership, without the use of intrusion detection schemes, and at the expense of moderate multi-path transmission overhead only. **Berman (2004)** in the paper "Enhancing Data Security in Mobile Ad Hoc Networks via Multipath Routing and Directional Transmission" a cross-layer approach is studied to improve data security in Mobile Ad Hoc Networks (MANETs). A thorough evaluation shows that these mechanisms can also improve data availability. In addition, this study presents a security-oriented analysis of several important design details that are associated with multipath message exchange.

Papadimitratos (2006) in the paper "Secure Data Communication in Mobile Ad Hoc Networks" address the problem of secure and fault-tolerant communication in the presence of adversaries across a multihop wireless network with frequently changing topology. To effectively cope with arbitrary malicious disruption of data transmissions, they propose and evaluate the secure message transmission (SMT) protocol and its alternative, the secure single-path (SSP) protocol.

Rachedi (2006) in the paper "A Secure Architecture for Mobile Ad Hoc Networks" proposed a new architecture based on an efficient trust model and clustering algorithm in order to distribute a certification authority (CA) for ensuring the distribution of certificates in each cluster. **Chasaki (2008**) in the paper "Topology Reconstruction via Path Recording in Secure MANET" provides a discussion of different path recording mechanisms. They evaluate their performance in terms of packet overhead and reconstruction complexity. **Luis et al. (2008)** in the paper "Securing the communication in Private Heterogeneous Mobile Adhoc Networks" proposed the method a pair-wise key based scheme for forming secured private clusters in mobile ADHOC networks. The solution tackles the problem of node authentication combined with traffic encryption in relatively small ADHOC networks using proactive

neighbour discovery and authentication. **M.A.Matin et al (2009)** in the paper "Performance Evaluation of Symmetric Encryption Algorithm in MANET and WLAN" proposed a method on symmetric encryption technique with AES algorithm in MANET and WLAN. Symmetric encryption is faster and requires less computational processing time. The increase in key size as well as block size, the security gets enhanced and linear cryptanalysis and differential cryptanalysis require more time to break the proposed cipher here. **Hongbo Zhou et al (2009)** in the paper "Secure auto configuration and Public key Distribution for Mobile Ad-hoc Networks" proposed a method of auto configuration which is a method to achieve uniqueness of address allocation with the help of IP address for each node. **Liebeherr (2009)** in the paper "An Overlay Approach to Data Security in Ad-Hoc Networks" shows that overlay networks can provide forward and backward secrecy for application data in an ADHOC network. **Mare.S.F. et al. (2011)** in the paper "Secret data communication system using stenography, AES and RSA" proposed a method that uses AES, RSA for securing sensitive data that assures integrity, authenticity and security. **Srivastava (2012)** in the paper "Secure Data Transmission in MANET Routing Protocol" focussed on achieving the routing and secure information exchange ensuring confidentiality, integrity and authentication of data exchange in a more suitable and secured way.

3. PROBLEM FORMULATION

A mobile ad hoc network (MANET) is a self-organizing system of mobile nodes. The nodes in MANET are free to move arbitrarily. The nature of the mobile ad hoc networks (MANETs) makes them very vulnerable to an adversary's security threats. Providing security through cryptographic algorithms in these networks is very important. Thus the objectives of problem formulation are:

- To develop a system those will Provide Security and Privacy to Data Transmission.
- To Establish a Secure System by using PGP & DES for protecting Sensitive data.

3.1 METHDOLOGY

To provide an information security in MANET, symmetric encryption algorithms play a main role among all the cryptographic algorithms. Encryption algorithms, used to provide information security, are known to be computationally intensive. This algorithm consumes a significant amount of computing resources such as memory, processing time and battery power. A mobile node, that consists of very limited resources, especially limited battery power, is subject to the problem of more energy consumption due to encryption algorithms. Designing a security algorithm requires an understanding of the common encryption schemes. This research work uses DES & PGP for encryption and decryption Algorithm in terms of security.

3.2 How DES works?

The Data Encryption Standard (DES) algorithm, adopted by the U.S. government in 1977, is a block cipher that transforms 64-bit data blocks under a 56-bit secret key, by means of permutation and substitution. DES works on bits, or binary numbers--the 0s and 1s common to digital computers. DES works by encrypting groups of 64 message bits, which is the same as 16 hexadecimal numbers. To do the encryption, DES uses "keys" which are also *apparently* 16 hexadecimal numbers long, or *apparently* 64 bits long. However, every 8th key bit is ignored in the DES algorithm, so that the effective key size is 56 bits. But, in any case, 64 bits (16 hexadecimal digits) is the round number upon which, DES is organized.

3.3 How PGP works?

PGP is a hybrid cryptosystem; it is a combination of some of the best known encryption algorithms in existence. While PGP has the speediness of a symmetric-key encryption algorithm, it maintains the high level of security of a public-key encryption algorithm.

The following algorithms are employed by PGP:

1. IDEA Cipher developed by James Massey & Xuejia Lai in 1990
2. RSA Public Key Encryption developed by Rivest, Shamir, and Adelman in 1977
3. GZIP is a combination of Lempel-Ziv and Huffman Encoding

About IDEA Cipher Algorithm:

1. IDEA: International Data Encryption Algorithm
2. Message is encrypted with a 128-bit IDEA key via different combinations of operations: a. Additions (mod 2^{16})

b. Multiplication(mod2^{16}+1)
c. Additions (mod 2) (i.e. XOR)

3. There are currently no known effective attacks against the IDEA cipher.

The IDEA cipher algorithm:

1. Original text is divided into 64-bit blocks.
2. Each 64-bit block is further divided into four 16-bit sub-blocks: X_1, X_2, X_3, X_4.
3. The 128-bit IDEA session key is divided into eight 16-bit key-blocks: $K_{i,1}$, $K_{i,2}$, $K_{i,3}$, $K_{i,4}$, $K_{i,5}$, $K_{i,6}$, $K_{i,7}$, $K_{i,8}$.
4. Addition and Multiplication are performed on each block of X_n and $K_{i,j}$.
5. The combinations of operations are performed eight times to get the final encryption.

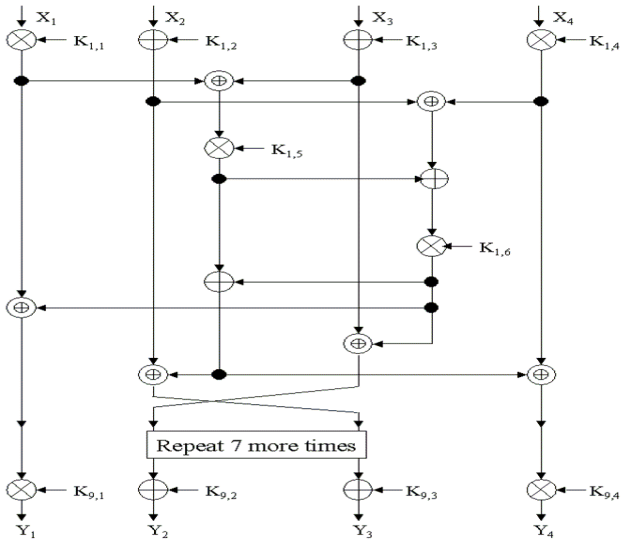

Fig 1: IDEA Algorithm

Problems with IDEA cipher:

1. IDEA is a symmetric-key cryptosystem. In order to decrypt a cipher, one must know the very same key that is used to encrypt the message.

2. Since the IDEA key is 128-bit long, it is not easy to memorize and therefore it must be recorded.

PGP Improvements:

1. Instead of using the same key each time, PGP randomly generated a new IDEA key for every session. The same message sent at different times will be totally different and remembering the key will be useless and unnecessary.
2. The IDEA key is encrypted via RSA public key encryption algorithm. Decryption can be achieved only by those who know the complementary key.
3. PGP compresses packages with GZIP.

How PGP Encrypts:

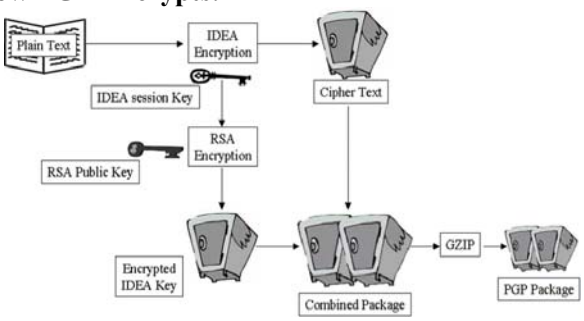

Fig 2: PGP Encryption

How PGP Decrypts:

1. PGP package is decompressed and is separated into the encrypted IDEA session key and the encrypted IDEA cipher text.
2. IDEA session key is decrypted with RSA private key.
3. IDEA session key decrypts the IDEA cipher text into the original plain text.

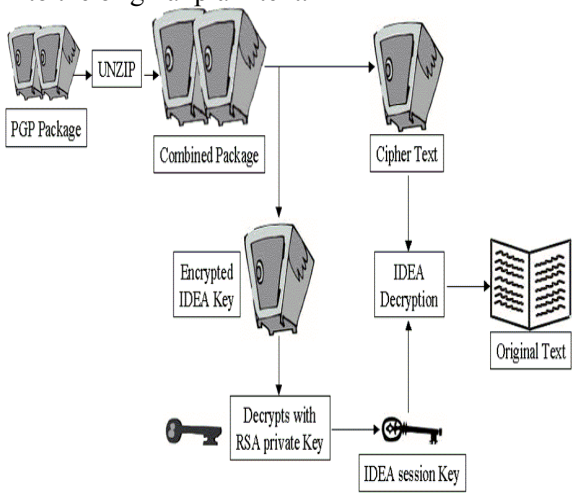

Fig 3: PGP Decryption

3.4 Why Choose PGP over IDEA & RSA?

RSA is very secured given a large enough key. However, it is very difficult to compute 567^2^{128} for every single letter in order to encrypt or decrypt a message. This complexity generated the need of a secure and compatible algorithm in form of PGP. It is fast, secured, best and easy to use. Although IDEA and RSA are very strong encrypting algorithms, they do have their weaknesses: IDEA uses a single and lengthy key while RSA employs complex and lengthy computations. By combining both IDEA and RSA, PGP uses the strengths of one algorithm to compensate for the weaknesses of the other. As the result, PGP is

one of the strongest and fastest encrypting algorithms in existence.

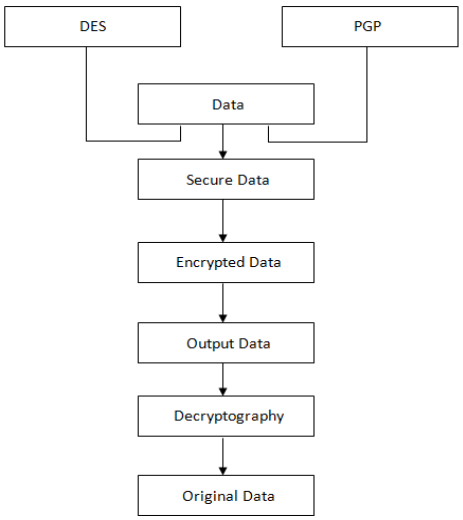

Fig 4: PGP & DES implementation

In the Proposed research work, PGP Encryption scheme with DES algorithm has been used to enhance the Security. The GUI model of proposed system was designed with the help of MATLAB Environment. In this model the data to be secured can be entered in the data section as shown in Fig 5.

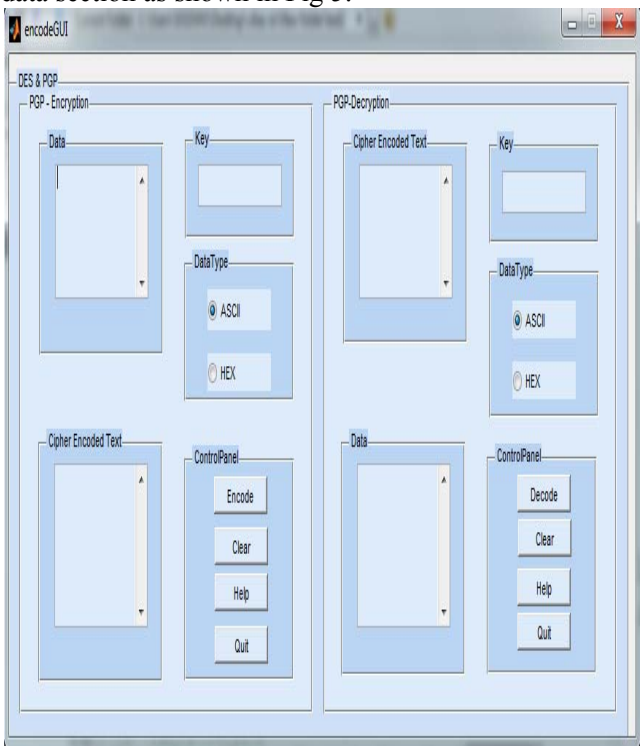

Fig 5 GUI model of Proposed System for Encryption Process

Figure 6 & 7 show the data used to be secured and the security key to be used. This key is 16 bit key either in ASCII or HEX for more security.

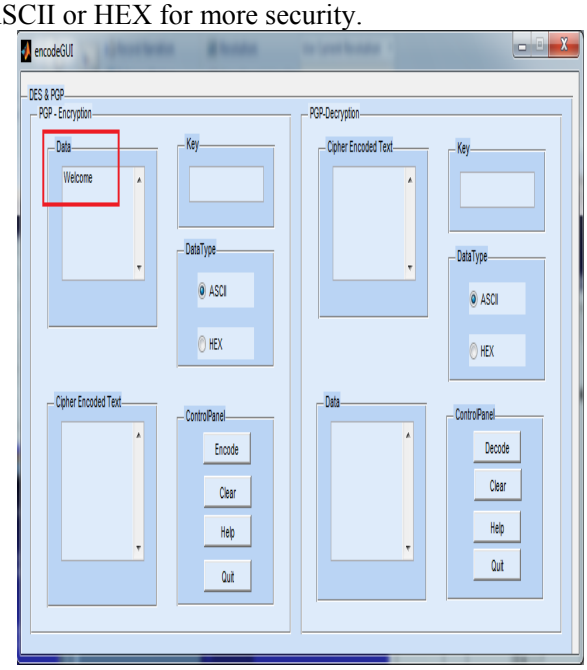

Fig 6: Data to be secured

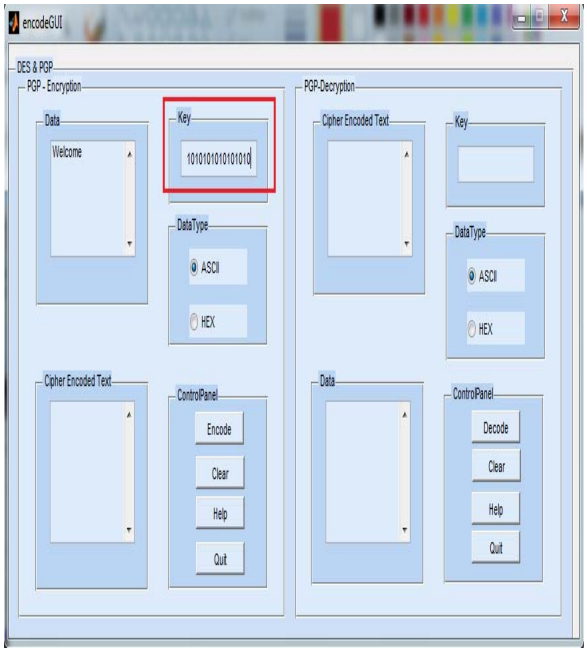

Fig 7 Key used

Figure 8 shows the method of encrypting the data by clicking on the encode button in the GUI model. It also shows the encoded text in the cipher encoded text Block.

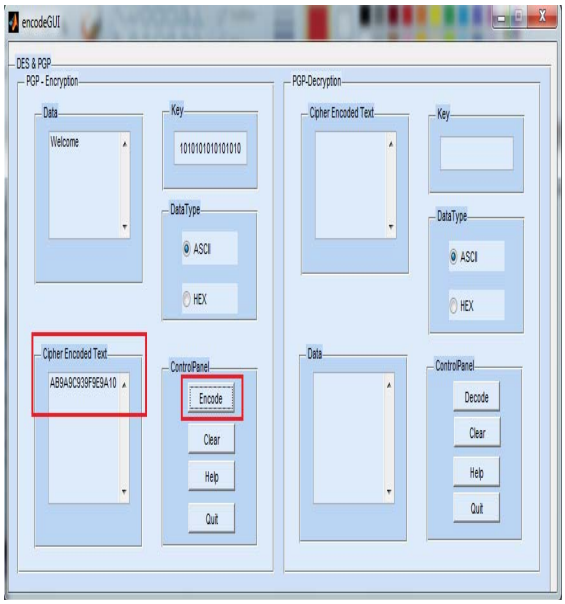

Fig 8: PGP Encryption (Cipher Encoded Text)

It gives cipher encrypted text using PGP & DES encryption scheme. This text must be used when the file is to be decrypted.

For Decryption process:

To decrypt data the cipher encoded text is used with 16-bit key as shown in figure 9 and decryption can be done by pressing decode button. It gives the original data that was secured by encryption.

Fig 9: PGP Decryption (Cipher Encoded Text)

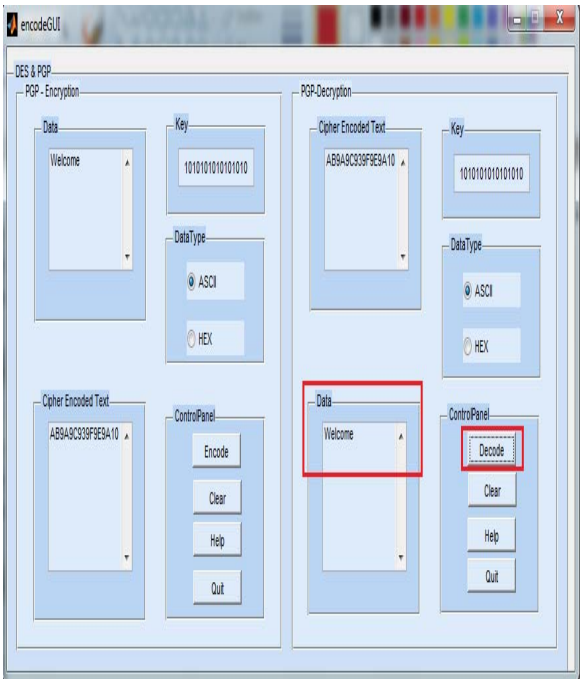

Fig 10: Retrieving of Original Data

Figure 10 shows that the original data has been retrieved on decoding the encrypted data using the same encryption key (used for encrypting the original data).

4. CONCLUSION

MANETs are much more vulnerable to attack than wired networks. The probable solution includes PGP & DES to determine the cipher encoded text of the original data. One key is used to protect data and that key is of 16-bit key. When user want to check the data then there is a need of one key & other is cipher encoded text which encrypted with the PGP Encryption & DES Encryption. Both work simultaneously. After encryption the data will be secured for future & can't be accessed by everyone. Because this key is not known and cipher encoded text can't be understand by anyone. This study has considered the hybrid system using PGP & DES encryption algorithm as a means of enhancing data security with respect to outsider attacks. Any scheme seeking to statistically improve data confidentiality and data availability with the use of multiple node-disjoint paths must consider the actual physical proximity of data transmissions on these paths. Hence, it has been found that existing schemes do not take full advantage of the security benefits fostered by multipath routing since they do not account

for physical and link layer details. In this method the PGP & DES are combined, to improve the security of such network. This secures the data as well as preserves the confidentiality.

5. FUTURE SCOPE

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defence mechanism. These factors have changed the battle field situation for the MANETs against the security threats. In future authentication schemes can be enhanced by using neural network associative memories to replace traditional authentication schemes.

REFERENCES

[1] Network Centric Warfare, Department of Defense, Washington, DC, Jul. 2001, report to Congress.

[2] Global Information Grid Architectural Vision, Department of Defense, Washington, DC, Jun. 2007.

[3] Renu Dalal,Yudhvir Singh and Manju Khar, "A Review on Key Management Schemes in MANET" International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012.

[4] Panagiotis Papadimitratos , Zygmunt J. Haas., "Secure message transmission in mobile ad hoc networks."

[5] Jorg Liebeherr and Guangyu Dong, "An Overlay Approach to Data Security in Ad-Hoc Networks"

[6] Danai Chasaki, Y. Sinan Hanay and Tilman Wolf, "Topology Reconstruction via Path Recording in Secure MANET" 978-1-4244-2677-5/08/$25.00 _c 2008 IEEE.

[7] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Data Transmission in Mobile Ad Hoc Networks" ACM Workshop on Wireless Security (WiSe 2003), San Diego, CA, September 19, 2003.

[8] Abderrezak Rachedi and Abderrahim Benslimane, "A Secure Architecture for Mobile Ad Hoc Networks" International Conference on Mobile Ad-hoc and Sensor Networks (MSN'2006), Hong Kong : China (2006) DOI : 10.1007/11943952_36.

[9] VLADIMIR BERMAN, "Enhancing Data Security in Mobile Ad Hoc Networks via Multipath Routing and Directional Transmission".

[10] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Data Communication in Mobile Ad Hoc Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006.

[11] Kartik Kumar Srivastava, Avinash Tripathi, and Anjnesh Kumar Tiwari, " Secure Data Transmission in MANET Routing Protocol" IJCTA , Int.J.Computer Technology & Applications,Vol 3 (6), 1915-1921 Nov-Dec 2012. Available online@www.ijcta.com

[12] Danai Chasaki and Tilman Wolf, "Evaluation of Path Recording Techniques in Secure MANET".

[13] Vineetha S. H. and Shebin Kurian, " Performance Analysis of Cluster Based Secure Multicast Key Management in MANET" **I**nternational **J**ournal of **C**omputer **S**cience and **T**elecommunications [Volume 4, Issue 4, April 2013].

[14] Ranjeet Singh, and Prof. Harwant Singh Arri, "COMPARISON OF AAMRP AND IODMRP USING SBPGP" International Journal of Computer Science and Management Research, Vol 2 Issue 3 March 2013.ISSN 2278-733X.

[15] Merin Francis, M. Sangeetha, and Dr. A. Sabari, "A Survey of Key Management Technique for Secure and Reliable Data Transmission in MANET" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013, ISSN: 2277 128X.

[16] J. Liebeherr, J. Wang, and G. Zhang. Programming overlay networks with overlay sockets. In Proc. 5th COST 264 Workshop on Networked Group Communications (NGC 2003), LNCS 2816, pages 242–253, Sep. 2003.

[17] H. Lundgren, E. Nordstrom, and C. Tschudin. Coping with communication grayzones in IEEE 802.11b. In Proc. of 5th ACM International Workshop on Wireless Mobile Multimedia (WoWMoM 2002), Sep. 2002.

[18] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang. Ursa: Ubiquitous and robust access control for mobile ad hoc networks. ACM/IEEE Transactions on Networking, 2005. To appear.

[19] C. E. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance vector routing (DSDV). In Proc. of ACM Sigcomm, pages 234– 244, Sep. 1994.

[20] C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100, Feb. 1999.

[21] T. Wolf, "A credential-based data path architecture for assurable global networking," in Proc. of the 2007 IEEE Conference on Military Communications (MILCOM), Orlando, FL, Oct. 2007.

[22] N. G. Duffield and F. Lo Presti, "Network tomography from measured end-to-end delay covariance," IEEE/ACM Transactions on Networking, vol. 12, no. 6, pp. 978–992, Dec. 2004.

[23] H. Tian and H. Shen, "Multicast-based inference of network-internal loss performance," in Proc. of 7th International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN 2004), Hong Kong, China, May 2004, pp. 288–293.

[24] V.N. Talooki, K. Ziarati "Performance comparison of routing protocols for Mobile Ad-Hoc Networks", Asia-Pacific conf. on Comm., APCC˝06.