A Comprehensive Survey on Cryptography Evaluation in Mobile (MANETs)

Suneetha Bulla[1], Pushya Chaparala[2], Samrajyam Mekala[3]

[1]Associate Professor, Dept. of CSE , KL Deemed to be University, suneethabulla@gmail.com
[2]Assistant Professor, Dept. of CSE , Vigna's Foundation of Science, Technology and Research, pushyachaparala@gmail.com
[3]Assistant Professor, Dept. of ECE , Vignan's Nirula Institute of Technology and Science for Women, samrajyamsuresh@gmail.com

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract – With the rapid development in network technology new network types based on wireless communication have emerged. A large family of wireless communication networks is the Mobile Ad hoc Networks (MANETs). While MANETs mobile devices should be able to connect with each other at any time and place, the vulnerabilities of MANET structure also introduce a wide range of attacks and present new challenges for the design of security mechanism ranging from developing and implementing lightweight cryptographic primitives to designing and analyzing secure protocols. Numerous security solutions and key management schemes such as symmetric and asymmetric cryptography have been used to support MANET environment. This paper conducted survey to gain a quick knowledge of security design demand and cryptography solutions to secure MANET. This survey focused on security schemas and case studies of cryptography techniques on Ad Hoc networks. Finally, conclusions are discussed.

Keywords: Ad Hoc Networks, security, Cryptography, Key management

1. Introduction

Now days, there is a massive change in communication technology due to usage of Internet Technology and handheld devices like laptops, smart phones, sensors etc. while transmitting and accessing data from one place to another place. Using these devices data can be transmitted anytime and anywhere since these devices support wireless communication. Hence wireless network communication plays vital role in our day to day life. The Ad Hoc networks can be classified into two categories such as resource dependent and resource less networks. Resource dependent networks are defined as cellular wireless networks and infrastructure fewer networks are defined as Ad Hoc wireless networks. The Ad hoc network has ability to dynamically configure them and establish among the routers shown as in figure 1.

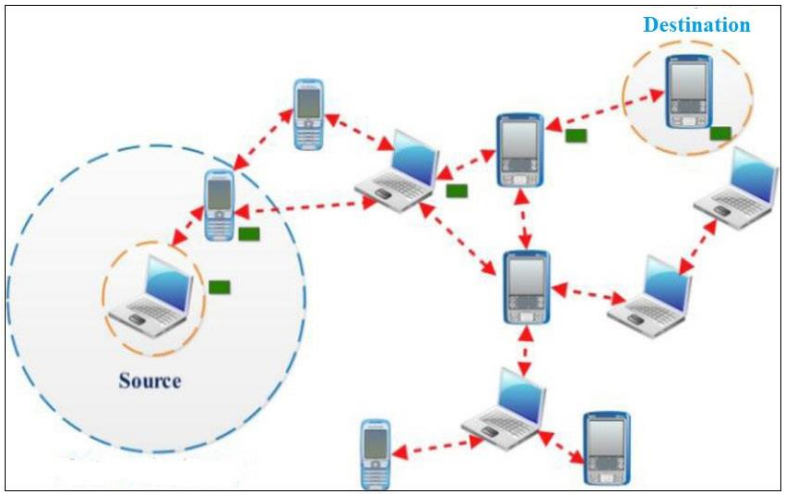

Fig.1. Basic architecture of Ad Hoc networks

Mobile Ad Hoc Network (MANET) is an independent set of self-organized communicating devices. The role of communicating device may be a network host or a network router. The communication between nodes through wireless links. MANETs do not maintain any fixed infrastructure and focal administration. Transmission capacity of the nodes is restricted. If any two mobile nodes are in same transmission range, one act as source and other act as destination then data can be transmitted directly from source to destination. This range is defined by the empowering technology via Zigbee, Bluetooth, Wi-Fi, and Medium Access protocols. If the source and destination nodes are not in same transmission range, intermediate nodes act as routers to transmit data from one hop to another. Therefore Mobile Ad Hoc Networks can be defined as fully distributed, autonomous, and cooperative communication networks. MANETs can be used in unreachable environments such

as fire detection, monitoring ocean depth and disaster recovery, battlegrounds, group meetings where participants assembled and transfer data among them with mobile devices in conference and symposium rooms and vehicle networks etc[1][2][3].

The major issues while designing Mobile Ad Hoc Networks are routing and providing Quality of Service (QoS). Due to the mobility nature of node and shared nature of wireless link, MANETs offering guaranteed QoS. The routing protocol also must provide certain level of QoS when required by a node during transmission. Throughput, Delay, Jitter, Bandwidth, Packet Delivery Ratio are parameters. The focus of cryptography and its basic applications in MANET will build the base for later research in security [4].

Cryptography is a Modern encryption technology it provides security of data midst of routers in Ad Hoc networks. It follows different statistical and mathematical modeling's of application or algorithms which was designed to provide security for communications. Cryptography [4] is defined as "the subdivision of cryptology in which encryption/decryption algorithms are designed, to guarantee the security and authentication of data". Cryptography algorithms classified into Symmetric and Asymmetric key. This paper conducted survey of MANET security and its implementation using cryptography; it can be better achieved with a broad knowledge. Various authors have contributed their extreme work on this area and this study focused on one-way hash functions, threshold cryptography, public key cryptography, identity-based cryptography, and signatures.

The rest of this paper is organized as follows; section II discusses about various authors contribution of security and Cryptography on MANETS. Section III Cryptographic techniques to secure MANET and demonstrates the related work in this field. Section IV contains the conclusion and future directions.

2. Security and Cryptography Background

Security architecture mainly focuses on security attacks, mechanisms, and services. These can be defined briefly as shown in TABLE I.

TABLE 1: SECURITY ARCHITECTURE

Security Service	Security Attack	Security Mechanism
Any process aims to enhance the security of the data processing or data transferring systems, and proposed to deal with security attacks using security mechanisms	Any action that compromises the information	Any process that can be used to detect, prevent, or recover from a security attack

Information security plays important roles it all measures taken to prevent unauthorized access whether this use takes the form of disclosure, alteration, substitution, or destruction. In this field it is a combination of processes, procedures, and systems used to ensure security services [4]. In this section a general overview of security services that applied for MANET which spread out from the traditional and well-known security services; confidentiality, authentication, integrity, availability, access control, and non-repudiation, which are defined as shown below.

a) Confidentiality: It is used to control access of sensitive information to prevent unauthorization. The MANET network uses an open medium, so usually all nodes within the transmission range can obtain the data. Only one way to protect data through encryption. Otherwise, may nodes have compromised by threads [4][5].

b) Authentication: The authentication is a service it concerned with assuring the message transmission from source to destination. However, there is no central authority in MANET, and it is very difficult to identify because of virtual connection. While confidentiality in MANET can be achieved via data encryption as mentioned before, authentication can be achieved by using textual code [6].

c) Data Integrity: The data integrity is an important parameter in the Ad HoC networks, it destroys customer data during transmission. It can be various forms duplication, insertion, alteration, reordering, or replays. Integrity in virtual medium, because the information can be changed by the attacker that was nabbed as replay attack. Hash functions shows solution to this situation and many authors are contributed there works [7].

d) Non-repudiation: it is an action on the node confirmed and associated with the customer. Signature based techniques are validated to use in MANETS. Private keys and public keys are uses in the cryptography to transmit data. In public key cryptography, users send data using its private key. All other nodes verifies A's public key, and A cannot deny that its signature is attached to the message [8].

Attacks in the MANET can be classified into two types passive and active based upon the source of the attack as internal or external and details are described in the below table in detailed. The passive attacks deal with eavesdropping on the transmission and at the same time traffic analysis and traffic monitoring also a solution. The table 2 classifies different passive and active attacks.

TABLE 2: Classification of Attacks

Passive Attack	**Active Attack**
Eavesdropping [10] Traffic Analysis or Traffic Monitoring [4]	Impersonation [10] Sinkhole Attacks [11] The Sybil Attack [11] Denial of Service (DoS) [12] Modification of Messages [11] Replay [11] Wormhole [10] Blackhole [10] Flooding Attack [5] Routing Table Poisoning Attack [10]

3. Cryptographic Techniques to Secure MANET

Security is plays main role in the WSN. There is a difficulty to identify which techniques are used to ensure the data transmission and which metrics are going to calculate the performance of the WSN. Cryptography is one of the techniques it is available in the form of symmetric and asymmetric. The first step may be is to choose when to use symmetric cryptography and to use asymmetric cryptography. Most of the research contributions are adopted asymmetric cryptography through RSA, digital signatures and so on in this field [11][8][13][14][15][16][17]. The cryptographic techniques used in select MANET security research work are shown in "Fig. 2". The details of the encryption schemes will be covered in this section. Many cryptographic techniques can be applied in MANET.

TABLE 3: HYBRID CRYPTOSYSTEM PROCESSES

Step	Description
1	Choose two integers in the source and destination nodes.
2	Calculate the public Keys for the source and destination nodes
3	Each node sends its public key to the other one
4	Calculate the shared secret key in both sender and receiver nodes using the public keys
5	Encrypt the data using the symmetric algorithm and the shared secret key in all data transferring between the source and destination nodes.

The main goal of the symmetric cryptography protecting data using secret key, which is used to encrypt and decrypt while hosting and retrieve data. In this cryptography secret key plays important role, in which the role of secret is encrypt and decrypt data between clients through public or private key to establish trust shaking. This technique is efficient than asymmetric in computational standpoint. More number of contributions are available and implemented different techniques and security solutions applied on the MANETs. Based on most of the contributed symmetric approaches are *Random Nonce [9], Shared Key [12] and HMAC message Authentication [19].*

Asymmetric cryptography is also called as public key cryptography and at the same time it is a combination of public key and private key, these are mentioned before. The private key is used to kept private data and public key can be public to the others. The well-known public key cryptographic techniques are the well-known DH and RSA algorithms, which were coming from 1970. Later many kinds of algorithms and techniques were implemented in the previous literature, such as digital signature, key management, and other techniques have been developed. In the public key cryptography, such as the El Gamal cryptograph system, DSA, and ECC. The asymmetric cryptography approaches are *Diffie-Hellman [16], Digital Signature Based on RSA/DSA [20][11], Identity-Based Cryptography (IBC) [21][22], Elliptic Curve Cryptography [13], Threshold and Identity-Based Cryptography [23][24], Hash Chain [25][26], Hybrid Cryptosystems [27].*

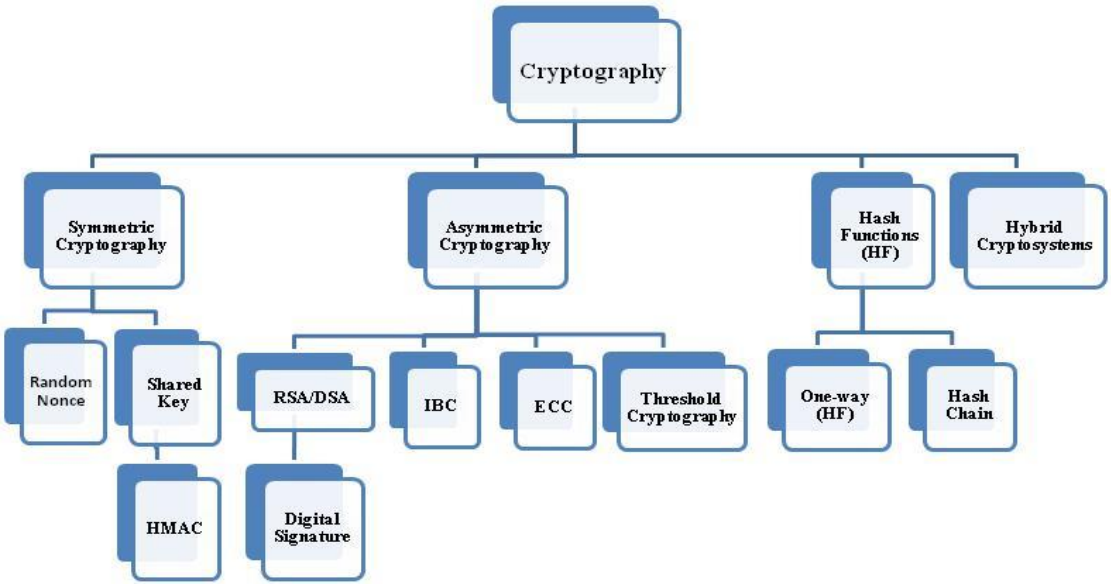

Fig. 2. Applied Cryptographic Techniques to Secure MANET

Symmetric vs Asymmetric Encryption

Many studies have compared asymmetric and symmetric encryptions based on properties of computational overhead, their simplicity of distributions. The symmetric encryption is faster than asymmetric encryption, so which consumes less CPU cycles when compare the asymmetric, Thus, from a speed point of view, symmetric is efficient than asymmetric encryption schemes. Even though, symmetric encryption generally has a many disadvantage. Here same key is used to encrypt and decrypt data while secure transmission [16]. The issue of securing symmetric key distribution becomes even more critical when the environment used for data transferring is vulnerable to security attacks. However, the asymmetric key encryption ensures private key secret, no one would be able to decrypt data. So, the public key can be easily distributed without worrying about the possibility of capturing it [29].

Related Work

This section discusses about various works on evaluation cryptography techniques performance on WSN. To protect MANET nodes from the attacker and the combination of robustness and enforcement methods are consider to more accurate methods. Many contributions are implemented distribution and lightweight methods to establish the trust between nodes without prior knowledge of the nodes [30]. In this section we will overview some research contributions in this field which applied to the different network layers of a MANET, and their primary goal is to protect or enforce the two basic functions.

Ahmad, at al. [1] and Mandal in [34] have conducted the complete analysis study of DES and conducted experiments using NS-2 simulator in terms of QoS metrics like of energy consumption, data transfer time, End-to-End delay time and throughput with varying data sizes. As per the simulation results the superiority of AES over DES performance metrics. So, the authors are recommended AES for their experiment. Ezeofor and Ulasi in [31] Jeeva, et al. [32] and presented an analysis of the most common data encryption algorithms DES, AES, Blowfish and RSA th at can be used in digital communication systems, where the data can be read, altered or forged by many types of attacks through unsecured paths. Abdul, et al. [33] and Singh and Maini in [37] provided an evaluation of six of the most common encryption algorithms: AES (Rijndael), DES, 3DES, RC2, Blowfish, and Rivest Cipher 6 (RC6). The comparison was done using different sizes and types of data blocks, different key size and different packet sizes.

Thakur and Kumar in [39] conducted comparison of different cryptography algorithms in the data encryption. They compared DES, Blowfish and AES with sleeted performance metrics to identify them. These are compared by behavioue and performance of the algorithms. The experiment was tested with different loads and different sizes of data. The algorithms were evaluated in terms of accuracy and time of encryption and decryption. The presented simulation results showed that Blowfish had a better performance than DES and AES encryption algorithms Mandal, et al. [40] discussed same works. Elminaam, et al. [41] and Nie, et al. [43] provided a comparison between the symmetric key encryption algorithms: DES, AES, and Blowfish using different data loads and conducted comprehensive survey. The simulation done using the provided classes in java environment to implement DES, AES and Blowfish. The simulation parameters were: speed, block size, and key size. Finally, the chosen metrics used to compare the performance of the algorithms were the algorithm's speed to encrypt and decrypt data blocks of various sizes.

Nadeem, and Javed in [42] evaluated and compared different encryption algorithms like DES, 3DES, AES and Blowfish. The performance of these algorithms compared by input file with different content of sizes on different hardware . Norouzi, et al. [46] implemented security algorithm in Ad hoc networks with predefined transmission rate. This experiment was simulated using MATLAB. Meanwhile for the second method data transmitted with three encryption algorithms: DES, AES and Blowfish. Thenmozhi and Madheswaran in [47] proposed a new method for different encryption algorithms (DES, AES, Blowfish and RC2) selection during processing of each packet instead of using a single encryption algorithm. The performance had been measured through simulation studies on NS-2.

Matin, et al., [48] and Elminaam et al., [49] examined the performance of a new cipher in MANET and wireless LAN networks and make a performance comparison with that of AES. The new proposed algorithm uses 200 bits key and its' performance had been evaluated algorithm in real network scenarios. Generally, a lot of researches have been done on evaluating the performance of some cryptographic mechanisms and encryption schemes to raise the data confidentiality in Table 4 we summarized the contributions in this field that we already detailed in this section.

TABLE 4: PERFORMANCE EVALUATION OF DIFFERENT ENCRYPTION SCHEMES CONTRIBUTIONS SUMMARY

The Author(s)	Analyzed Algorithm(s)	Factor(s)	Simulator	Metric(s)	OSI Layer in which Algorithms Examined	Recommended Algorithm Among Selected
Khan, et al. (2017)	DES, 3DES, AES and Blowfish	Encryption Algorithms	Special software (the authors did not mentioned the used network simulator)	Data encryption time, throughput and energy consumption	Application and network layers	Blowfish

Ahmad, et al. (2015)	AES, DES, 3DES and DH	Encryption Algorithms Number of hops Data file size Simulation modes including or excluding DH	NS-2	Data transfer time Energy consumption Network throughput	Application and network layers	DES
Ezeofor and Ulasi (2014)	DES, AES, Blowfish and RSA	Different data block sizes	Visual basic based simulation program	Processing time	Application and network layers	RSA
Jeeva, et al. (2012)	AES, RSA, DES, 3DES, DSA and RC2	The key length	Visual basic based simulation program	Tunability and the computational speed	Application and network layers	AES among symmetric RSA among asymmetric
Abdul, et al. (2009)	AES, DES, 3DES, RC2, Blowfish and RC6	Different data block sizes Different data block types Different key sizes	Network simulator (not specified)	Encryption time CPU processing time Power consumption	Application layer	Blowfish
Mandal, (2012)	AES, DES, 3DES and Blowfish	Different data block sizes Different key sizes	Java programming based simulation program	Encryption time CPU processing time Network throughput Power consumption	Application layer	Blowfish
Masram, et al., (2014)	AES, DES, 3DES, RC2, Blowfish, Skipjack and RC4	Different data block sizes Different data block types Different key sizes	Java Cryptography Extension	Encryption time	Application layer	RC4
Elminaam, et al., (2009)	AES, DES, 3DES, RC2, Blowfish and RC6	Different data block sizes Different data block types Different key sizes	.NET environment	Encryption time	Application layer	Blowfish
Singh and Maini (2011)	AES, DES, 3DES and Blowfish	Different data block sizes	C# based simulation program	Encryption time Network throughput	Application layer	Blowfish
Kumar and Karthikey	Blowfish and Rejindael	Different data block sizes Different data	Not specified	Energy consumption	Application layer	Blowfish

an (2012)		block types Different key sizes				
Thakur and Kumar (2011)	DES, 3DES and Blowfish	Different data block sizes	C# based simulation program	Encryption speed Efficiency against attacks	Application layer	Blowfish
Mandal, et al., (2012)	DES and AES	Different data block sizes	MATLAB	Encryption time Memory usage	Application layer	AES
Elminaam, et al., (2010)	DES, AES and Blowfish	Different data block sizes Different key sizes	Java Cryptography Extension	Encryption time	Application layer	Blowfish
Nadeem and Javed (2005)	DES, AES, 3DES and Blowfish	Different data block sizes Different hardware platforms	Java platform (JDK 1.4)	Encryption time	Application layer	Blowfish
Nie, et al. (2014)	CAST, Blowfish, RC5 and AES	Different Ciphers	External workstation	Run time Memory utilization Power consumption	Physical layer	Blowfish
Umaparvathi and Varughese (2010)	DES, AES, 3DES and Blowfish	Different data block types	Java programming based simulation program	Encryption time Power consumption	Application layer	AES
Sahu and Kushwaha (2014)	DES, AES and Blowfish	Different data block types Different data block sizes	NS-2	Encryption time Power consumption	Application layer	AES
Norouzi, et al., (2012)	DES, AES and Blowfish	Different data block types	MATLAB	Encryption time Network throughput	Application layer	AES
Thenmozhi and Madheswaran (2012)	DES, AES, RC2 and Blowfish	Different data block types Different data block sizes	NS-2	Average delay time Average jitter Network throughput	Application and network layers	Blowfish
Matin, et al., (2009)	New cipher based on AES and AES itself	Different data block size	Real network	Matin, et al., (2009)	New cipher based on AES and AES itself	Different data block size
Elminaam, et al., (2008)	AES, DES, 3DES, RC2, Blowfish, and RC6	Different data block types Different data block sizes	Not specified	Encryption time CPU process time CPU clock cycles	Application layer	Blowfish

				Battery power		
Yao et al., (2013)	RSA, ELG, DES, ECC, AES, IDEA, MD5, CAESAR, SHA1 and BASE64	Different data block types Different data block sizes	JDK software	Percentage of battery power Battery voltage Battery temperature	Application layer	AES
Othman et al., (2012)	AES, RC5 and RC6	Different ciphers Different key sizes	Mica 2 sensor small nodes (motes)	Memory usage Energy consumption Process time	Application, network and physical layers	RC5
Stewart et al., (2005)	A new proposed encryption scheme	Number of nodes Number of routes	Special hardware	Secrecy of the data Power consumption	Application and network and physical layers	The new proposed encryption scheme
Papaj et al., (2011)	A new integration security model	Number of nodes	OPNET modeler	Total packet processing delay time	Physical and network layers	The new integration security model
Juwad and Al-Raweshidy (2008)	Proposed Secure-AODV (SAODV)	AODV vs SAODV With vs Without attach	OPNET modeler	Average TCP throughput Routing control overhead	Application and network layers	SAODV
Kumar and Aggarwal (2012)	ECC	Different elliptic curves	Special software	Packets drop Network throughput End to End delay Jitter	Application and network layers	Weierstrass form ECC

4. Conclusions and future directions

Security of Ad Hoc networks is one of the research topics in the advanced technology updates. As per the previous literatures [56][57][58] cryptography is one of the solutions to provide security in MANETs. It reduce the computation cost, improving security and improving key management techniques. This paper conducted survey on the security and cryptography issues in MANETs. The objective of this paper can be twofold, preventing different types of attacks and cryptography implementation in MANETs. We are classified attacks into two types active and passive and explained with internal and external details. Second part of this paper discussed about cryptography and its implementation on MANETS. The cryptographic techniques always play a major role in the design of each stage of the key management. The security solution applied for MANET will always be under spot by the research community and the new design will come out quickly and easily reusable as popular design patterns using cryptography terminologies [58]. Finally identified few most relevant contributions to compare with existing literatures. DES, Blowfish, AES are most frequently used cryptography algorithms in the MANET security.

References

1. Ahmad, A., Swidan, A., & Saifan, R. (2015) Comparative Analysis of Different Encryption Techniques in Mobile Ad hoc NETworks (MANETS). International Journal of Computer Networks & Communications (IJCNC).
2. Akbani, R. Korkmaz, T. and Raju, G. V. S. (2012), Mobile Ad-Hoc Networks Security. In Recent Advances in Computer Science and Information Engineering, Springer Berlin Heidelberg, 659-666.
3. Masoud, M., Jannoud, I., Ahmad, A., & Al-Shobaky, H. (2015, September). The power consumption cost of data encryption in smartphones. In Open Source Software Computing (OSSCOM), 2015 International Conference on (pp. 1-6). IEEE.
4. Meyer, C. (1989, May). Cryptography-A state of the art review. InCompEuro'89.,'VLSI and Computer Peripherals. VLSI and Microelectronic Applications in Intelligent Peripherals and their Interconnection Networks', Proceedings. (pp. 4-150). IEEE.
5. Agrawal, S. Jain, S. and Sharma, S. (2011), A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks. arXiv preprint, arXiv:1105.5623.
6. Menezes, A. J. Van Oorschot, P. C. and Vanstone, S. A. (1996), Handbook of applied cryptography. CRC press.
7. Malathi, M. Divya, P.S. Anusha, M. and Rajalakshmi, K. (2012), Multilevel Authentication for Vehicular Ad-Hoc Networks with Cryptography Hash Functions. Radar, Communication and Computing (ICRCC), International Conference.
    a. Sharma, P. and Trivedi, A. (2011), An Approach to Defend Against Wormhole Attack in Ad hoc Network Using Digital Signature. In Communication Software and Networks (ICCSN), 2011 IEEE Third International Conference, 307-311.
8. Chen, J. and Wu, J. (2010), A Survey on Cryptography Applied to Secure Mobile Ad hoc Networks and Wireless Sensor networks. Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice, IGI Global, AH ALTALHI, 5, 2414-2424.
9. El-Mousa, A. and Suyyagh, A. (2010), Ad hoc Networks Security Challenges. In Systems Signals and Devices (SSD), 2010 IEEE Seventh International Multi-Conference, IEEE, 1-6.
10. Benamar, K. (2007), the Adaptation of Security Mechanisms for Ad hoc Networks. Unpublished Master Thesis, University of Abou Bekr Belkaid, Algeria.
11. Matin, M. A. Hossain, M. M. Islam, M. F. and Islam, M. N. (2009), Performance Evaluation of Symmetric Encryption Algorithm in MANET and WLAN. In Technical Postgraduates (TECHPOS), International Conference, IEEE, 1-4.
12. Liu, A. and Ning, P. (2008), TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks. In Information Processing in Sensor Networks, IPSN'08. International Conference.IEEE, 245-256.
13. Aware, A. A. and Bhandari, K. (2014), Prevention of Black Hole Attack on AODV in MANET Using Hash Function. In Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2014 3rd International Conference, IEEE, 1-6.
14. Clausen, T. H. Dean, J. W. and Dearlove, C. (2011), Mobile Ad hoc Network (MANET) Neighborhood Discovery Protocol (nhdp). Naval Research.
15. Stulman, A. Lahav, J. and Shmueli, A. (2013), Spraying Diffie-Hellman for Secure Key Exchange in MANETs. In Security Protocols XXI, Springer Berlin Heidelberg, 202-212.
16. Yang, H. Luo, H. Ye, F. Lu, S. and Zhang, L. (2004), Security in Mobile Ad hoc Networks: Challenges and Solutions. Wireless Communications, IEEE, 11(1), 38-47.
17. Singh, A. Maheshwari, M. and Kumar, N. (2011), Security and Trust Management in MANET. In Information Technology and Mobile Communication, Springer Berlin Heidelberg, 384-387.
18. Clausen, T. H. Dean, J. W. and Dearlove, C. (2011), Mobile Ad hoc Network (MANET) Neighborhood Discovery Protocol (nhdp). Naval Research.
19. PUB, F. (2000). Digital Signature Standard (DSS).
20. Zhao, S. Aggarwal, A. Frost, R. and Bai, X. (2012) A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks. Communications Surveys & Tutorials, IEEE, 14(2), 380-400.
21. Xia, P. Wu, M. Wang, K. and Chen, X. (2008), Identity-Based Fully Distributed Certificate Authority in an OLSR MANET. In Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference, IEEE, 1-4.
22. Kush, A. (2008), Review of Hashing as Security Tool in Wireless Ad Hoc Networks.
23. Huang, Q. Cao, R. Deng, B. and Wang, X. (2011), Hash-chain Based Public Key Management Algorithm of Mobile Ad hoc network. In Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on, IEEE, 1, 247-251.

24. Irshad, A. Gilani, S. M. Khurram, S. Shafiq, M. Khan, A. W. and Usman, M. (2010), Hash-Chain Based Peer-Peer Key Management and Establishment of Security Associations in MANETS. In Information and Emerging Technologies (ICIET), 2010 International Conference, IEEE, 1-6.
25. Ullah, I., Abbas, G., & Abbas, Z. H. (2017, November). Energy-aware congestion-less dynamic source routing for MANETs. In Multi-topic Conference (INMIC), 2017 International (pp. 1-6). IEEE.
26. Sivaranjani, S. and Rajashree, S. (2014), Secure Data Transfer in MANET Using Hybrid Cryptosystem. In Information Communication and Embedded Systems (ICICES), International Conference, IEEE, 1-5.
27. Villanueva, J. C. (2015), Symmetric vs Asymmetric Encryption. From http://www.jscape.com/blog/bid/84422/Symmetric-vs-Asymmetric-Encryption.
28. Sasi, S. B. Dixon, D. Wilson, J. and No, P. (2014), A General Comparison of Symmetric and Asymmetric Cryptosystems for WSNs and an Overview of Location Based Encryption Technique for Improving Security. IOSR Journal of Engineering, 4(3), 1.
29. Marias, G. F., Georgiadis, P., Flitzanis, D., & Mandalas, K. (2006). Cooperation enforcement schemes for MANETs: A survey. Wireless Communications and Mobile Computing, 6(3), 319-332.
30. Ezeofor, C. J. and Ulasi, A. G. (2014), Analysis of Network Data Encryption & Decryption Techniques in Communication Systems. International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), 3(12).
31. Jeeva, A. Palanisamy V. and Kanagaram K. (2012), Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms. International Journal of Engineering Research andApplications (IJERA), 2(3).
32. Abdul, D. S. Elminaam, H. M. A. K. and Hadhoud, M. M. (2009), Performance Evaluation of Symmetric Encryption Algorithms. International Journal of Computer Science and Network Security, 8(12), 78-85.
33. Mandal, P. C. (2012), Evaluation of Performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish. Journal of Global Research in Computer Science, 3(8), 67-70.
34. Masram, R. Shahare, V. Abraham, J. and Moona, R. (2014), Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based on Various File Features. International Journal of Network Security & Its Applications, 6(4).
35. Elminaam, D. S. Kader, H. M. A. and Hadhoud, M. M. (2009), Energy Efficiency of Encryption Schemes for Wireless Devices. International Journal of Computer Theory and Engineering, 1, 302-309.
36. Singh, S. and Maini, R. (2011), Comparison of Data Encryption Algorithms. International Journal of Computer Science and Communication, 2(1), 125-127.
37. Kumar, M. A. and Karthikeyan, S. (2012), Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms. International Journal of Computer Network and Information Security (IJCNIS), 4(2), 22.
38. Thakur, J. and Kumar, N. (2011), DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. International journal of emerging technology and advanced engineering, 1(2), 6-12.
39. Mandal, A. K. Parakash, C. and Tiwari, A. (2012), Performance Evaluation of Cryptographic Algorithms: DES and AES. In Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference, IEEE, 1-5.
40. Elminaam, D. S. A. Abdual-Kader, H. M. and Hadhoud, M. M. (2010), Evaluating the Performance of Symmetric Encryption Algorithms. IJ Network Security, 10(3), 216-222.
41. Nadeem, A. and Javed, M. Y. (2005), A Performance Comparison of Data Encryption Algorithms. In Information and communication technologies. ICICT 2005. First international conference, IEEE, 84-89.
42. Nie, T. Zhou, L. and Lu, Z. M. (2014), Power Evaluation Methods for Data Encryption Algorithms. Software, IET, 8(1), 12-18.
43. Umaparvathi, M. and Varughese, D. K. (2010), Evaluation of Symmetric Encryption Algorithms for MANETs. In Computational Intelligence and Computing Research (ICCIC), IEEE International Conference, 1-3.
44. Sahu, S. K. and Kushwaha, A. (2014), Performance Analysis of Symmetric Encryption Algorithms for Mobile Ad hoc Network. In International Journal of Emerging Technology and Advanced Engineering IJETAE, 4(6).
45. Norouzi, M. esmaeel Akbari, M. and Souri, A. (2012), Optimization of Security Performance in MANET. Journal of American Science, 8(6).
46. Thenmozhi, N. and Madheswaran, M. (2012), Dynamically Changing the Symmetric Encryption Algorithm for Improving Security and Performance during Data Transfer in Grid Networks. International Journal of Computer Applications, 55(7), 22-27.
47. Matin, M. A., Hossain, M. M., Islam, M. F., Islam, M. N., & Hossain, M. M. (2009, December). Performance evaluation of symmetric encryption algorithm in MANET and WLAN. In Technical

Postgraduates (TECHPOS), 2009 International Conference for (pp. 1-4). IEEE.
48. Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2008). Performance evaluation of symmetric encryption algorithms. IJCSNS International Journal of Computer Science and Network Security, 8(12), 280-286.
49. Yao, H., Lian, L., Fan, Y., Liang, Q., & Yan, X. (2013, December). The Evaluation of Security Algorithms on Mobile Platform. In Mobile Ad-hoc and Sensor Networks (MSN), 2013 IEEE Ninth International Conference on (pp. 405-409). IEEE.
50. Othman, S. B., Trad, A., & Yo, H. (2012, March). Performance evaluation of encryption algorithm for wireless sensor networks. In Information Technology and e-Services (ICITeS), 2012 International Conference on (pp. 1-8). IEEE.
51. Stewart, K., Haniotakis, T., & Tragoudas, S. (2005, March). Design and evaluation of a security scheme for sensor networks. In Sixth international symposium on quality electronic design (isqed'05) (pp. 197-201). IEEE.
52. Kumar, A., & Aggarwal, A. (2012, February). Performance analysis of MANET using elliptic curve cryptosystem. In Advanced Communication Technology (ICACT), 2012 14th International Conference on (pp. 201-206). IEEE.
53. Papaj, J., Čižmár, A., & Doboš, Ľ. (2011, June). Implementation of the new integration model of security and QoS for MANET to the OPNET. In International Conference on Multimedia Communications, Services and Security (pp. 310-316). Springer Berlin Heidelberg.
54. Juwad, M., & Al-Raweshidy, H. S. (2008, May). Experimental Performance Comparisons between SAODV & AODV. In 2008 Second Asia International Conference on Modelling &# x00026; Simulation (AMS) (pp. 247-252). IEEE.
55. Mandala, S., Ngadi, M. A., & Abdullah, A. H. (2007). A survey on MANET intrusion detection. International Journal of Computer Science and Security, 2(1), 1.
56. Mamatha, G. S., & Sharma, D. S. (2010). Network Layer Attacks and Defense Mechanisms in MANETS-A Survey. International Journal of Computer Applications (0975–8887) Volume.
57. Manikandan, K. P., Satyaprasad, D. R., & Rajasekhararao, D. K. (2011). A survey on attacks and defense metrics of routing mechanism in mobile ad hoc networks. IJACSA) International Journal of Advanced Computer Science and Applications, 2(3).
58. Marias, G. F., Georgiadis, P., Flitzanis, D., & Mandalas, K. (2006). Cooperation enforcement schemes for MANETs: A survey. Wireless Communications and Mobile Computing, 6(3), 319-332.
59. Rajankumar, P., Nimisha, P., & Kamboj, P. (2014, March). A comparative study and simulation of AODV MANET routing protocol in NS2 & NS3. In Computing for Sustainable Global Development (INDIACom), 2014 International Conference on (pp. 889-894). IEEE.
60. Tan, S., & Kim, K. (2013, November). Secure Route Discovery for preventing black hole attacks on AODV-based MANETs. In High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference on (pp. 1159-1164).