International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Cryptography Techniques based on Security of AODV in MANETs - A Survey

Ankita Singh[1], Mahima Sharma[2]

School of Computing Science & Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India

Abstract: ***Network's popularity and demand has motivated the development of mobile adhoc networks (MANETs).MANETs are a kind of wireless adhoc network which is infrastructure less. Each device or nodes are free to move independently in any random direction due to this links between the devices is not constant.This dynamic nature of network topology makes security issues more complex. In this paper, we discuss the solutions for security threats in AODV protocol. Security threats like wormhole attack, black hole attack, eaves dropping etc can defended by using cryptographic techniques like RSA, DES, AES. Main issues with security mechanisms that are available is their effect on performance of algorithm like more processing power, packet drop, throughput etc. Finally, concluding over the solutions for security through these algorithms so that performance and security can be enhanced in future.***

Keyword: MANET; adhoc ; AODV; AES;DES;RSA

1. Introduction

A wireless adhoc network is temporarily set network by wireless mobile computers moving arbitrary in the place that have no fixed infrastructure and all of the transmission links are established through wireless medium. MANETs are a kind of wireless adhoc network. Each node in a MANET is free to move independently in any direction leads to changing its links to other nodes frequently. Due to their self- organizing nature they do not require expensive fixed infrastructures. Evidently, these types of networks are more vulnerable to threats because of dynamic topology. In ad hoc networks, routing protocols are categorized in two groups; the reactive routing protocols and proactive routing protocols. Among the MANET routing protocols, reactive routing protocols have gained more attention; a reactive routing protocol discovers a route only when needed. This enables a reactive routing protocol to achieve better performance than the proactive routing protocols, which discovers and maintains all possible routes in the network even though they may never be used.

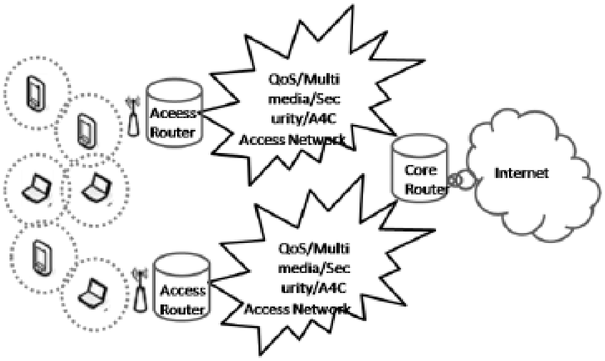

QoS/Multi media/Sec urity/A4C Access Network
Aceess Router
Core Router
Internet
QoS/Multi media/Sec urity/A4C Access Network
Access Router

Figure 1: Mobile Adhoc Network

AODV routing protocol is an improvement of DSDV, it typically minimizes the number of required broadcast by creating routes if it is required, not as in DSDV in which maintaining a complete list of routes is done. AODV does not specify any special security measures and is vulnerable to many types of attacks that manipulate its routing control mechanism. Among the attacks to AODV routing protocol is the black hole attack, so the black hole node can disrupt network operations and disobey the AODV routing specification. These threats make this protocol less reliable.

2. Routing in MANETS

In MANETs each node works as a router by which overhead of routing get reduced compared to wired networks. Nodes can communicate with each other if they are in communication range of each other; if they are not then the sender sends message through intermediate nodes.

As nature of MANETs is unpredictable and dynamic nodes do not have prior knowledge about topology due to which nodes has identify the efficient topology to start the transmission.

Role of routing protocol is even more challenging in the case of MANETs routing, as it has various constraints with vibrant topology which makes it complex to manage.

The primary goal of any routing protocol is to set up an optimal route which has minimal overhead and consumes minimum bandwidth possible.

MANET routing protocols are categorized in three categories:

- Proactive
  Routes are computed prior to requirement.
  Periodical update and distribution of routing information is performed. Example- DSDV, OLSR, WRP, CGSR, FSR
- Reactive
  Routes are discovered when in demand.
  No requirements of distribution of routing information.
  Example-AODV, DSR, ACOR, ABR
- Hybrid
  A combination of benefits of proactive and reactive protocol is implemented.
  Example- TORA, ZRP, ARPAM, OORP, HSR, CGSR, LANMAR.

Proactive protocol has advantage of selecting route immediately when required without holding. But it has drawback of higher bandwidth and slow reaction on failures. Reactive protocol consumes less bandwidth and effective in routing. Drawback is it takes higher time for route discovery and sometimes congestion is faced when flooding requests are received. Efficiency of hybrid protocol depends on the number of nodes and the amount of traffic decides the reaction to requests received.

3. Adhoc on Demand Vector protocol (AODV)

AODV is a reactive type of routing protocol in MANETs. Route discovery is not initiated until it is required (on-demand), the protocol operates in two phases: Route Discovery and Route Maintenance. Route discovery is used when a source node want to send message to a target node without the routing, it sends/broadcast RREQ first. When the adjacent node received RREQ with the addresses of source node and target node, before forwarding, it keeps a reverse path to the source node in its routing table. The routing table records the route information of the next hop, the distance and the current highest sequence number it has seen then it judges if it was the same with the target node's address. If it was, then it sends the RREP to source node, otherwise, checking the routings in the rout table that could reach the target node, then it sends RREP to source node, or continue to flooding sent RREQ. Source node receives multiple RREP packets via different paths. Source node selects fresher and shorter path among them to send the application data. AODV protocol maintains routing nodes through broadcasting hello message regularly. If one link breaks, it sends ERROR message to nodes, meanwhile deleting broken records or repairing the routing.

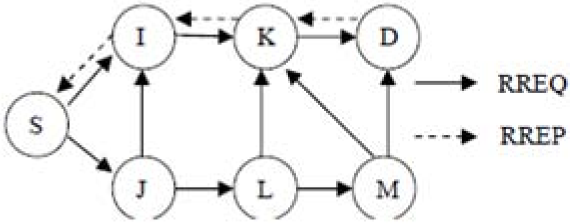


Figure 2: Route Discovery Process of AODV Routing Protocol

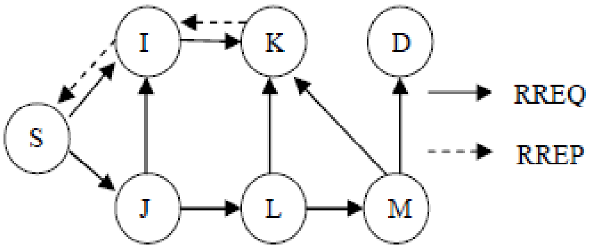


Figure 3: Route Reply Process Of AODV Routing Protocol

Once the source node receives the correct RREP message then the data transmission starts. With the intention of speeding up the Route Discovery process, AODV also allows the intermediate nodes which have the route to the targeted destination node to generate a RREP message and send it back to source node again.

4. Security Goals and Attacks

Information or data in network is an asset which needs to be secured from attacks. Information needs to be protected from unauthorized access (confidentiality), protected from unauthorized change (integrity)and available to legal users when it is demanded (availability).Security goals are as follows:

Confidentiality: privacy of information is kept from false users. When piece of information is send, it has to be conceal while transmission.

Integrity: Integrity means that changes in data need to be done by authorized entities. Information should not be spoiled during transmission.

Availability: The information should be available to authorized users. Assuring the network service is also available to all authorized users.

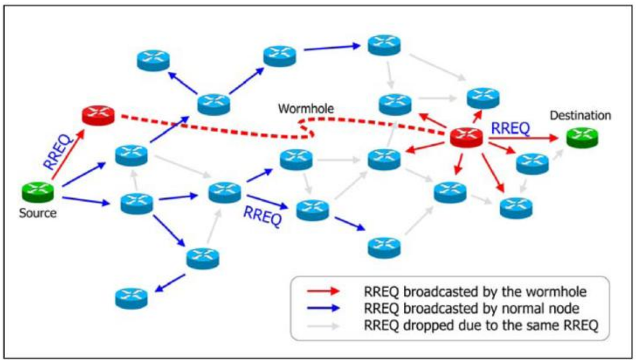

Wormhole
Destination
RREQ
RREQ
Source
RREQ
RREQ broadcasted by the wormhole
RREQ broadcasted by normal node
RREQ dropped due to the same RREQ

Figure 4: Attacks in MANETs

Attacks in MANETs

- Internal Attacks: Attackers act as one of the nodes among other nodes. Attacker's gains direct access to the network by impersonation of a proper node and then it perform malicious activities.
- External attacks: Attackers attack from outside the network, it causes congestion in the network by propagating non meaningful message throughout the network, and then it disturbs the whole communication.

Some other types of attacks are:-

a) Impersonation: The attacker can act as a normal node and joins the network and can harm the network. Several this kind of nodes altogether can have control over a whole network and conduct malicious behaviour.
b) Denial of service: Malicious nodes generate false messages in order to disrupt the network's operation and they consume other node resources.
c) Wormhole attack: This kind of attack is launched by two malicious nodes (worms) connected via a high speed wired or wireless link called wormhole link or tunnel. Then communication of outside nodes is done via this tunnel by multi hop, they encapsulate data packets and falsify the route length.

d) Black hole attack: The attack is created at main centre of network. It traps the traffic; it then attracts the nodes by offering attractive paths to the neighbouring nodes.

e) Eavesdropping: Goal of attacker is to retrieve private information while transferring through network from node to other. Private information like keys and passwords are being targeted mainly in this kind of attack.

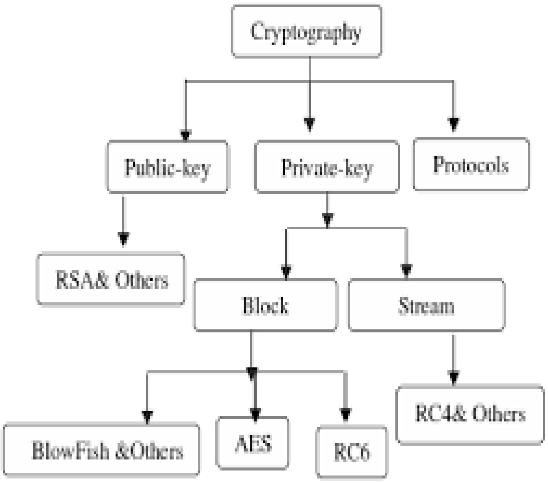


Figure 5: Cryptography Techniques

5. Cryptographic Techniques for security in MANETs

Cryptographic mechanism can be considered as the most reliable technique to guarantee integrity, availability and confidentiality by key management. An original message (plain text) is converted into cipher text by process of encryption at sender side then restoring the plain text from cipher text is done by decryption process at receivers end. Scheme used for encryption constitute the area of study known as cryptography. Cryptographic techniques are categorized into two types.

Cryptographic techniques:

- Private key cryptography:
  The same shared secret key is used for both encryption and decryption at sender's and receiver's end respectively. It is also known as symmetric key cryptography. Every pair of communicating nodes share a secret key, which means that for n entities to communicate securely, the number of keys required is K=n*(n-1)/2.
  Some of the algorithms which come under this category are AES, DES, DEA, RC2, BLOWFISH etc.

- Public key cryptography:
  Two different keys are required in this technique for each node. A public key is used to encrypt the message at sender's end and a private key is used to decrypt the message at receiver's end. It is also called asymmetric key cryptography. This technique requires fewer unit of keys compared to symmetric key cryptography, the number of keys is K=2*n, for n communicating nodes. Some of the algorithms which are included in this category are RSA, Diffie-Hellman key agreement and Digital signature algorithm.

1. Symmetric Key algorithms:

a) Advanced Encryption Standard (AES)

AES technique is not only used for securing but also for high speed. Encrypts data blocks of 128 bits in 10, 12, 14 rounds depending on key size.

AES is fast and flexible. It can be made run on various platforms especially on small devices.

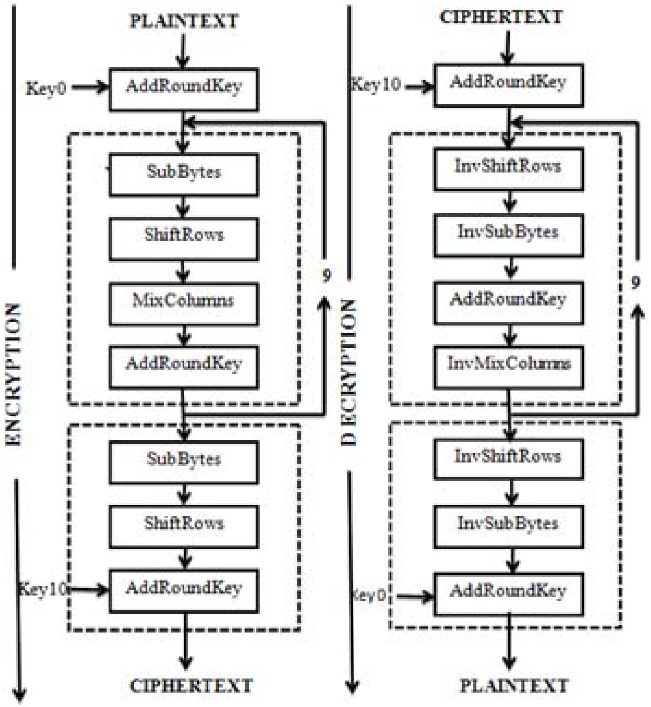


Figure 6: AES Encryption and Decryption

i. ***Algorithm Steps*: These steps used to encrypt 128-bit block**

1. The set of round keys from the cipher key.
2. Initialize state array and add the initial round key to the starting state array.
3. Perform round = 1 to 9: Execute Usual Round.
4. Execute Final Round.
5. Corresponding cipher text chunk output of Final Round Step

ii. Usual Round :

Execute the following operations which are described above.

1. Sub Bytes
2. Shift Rows
3. Mix Columns
4. Add Round Key, using K (round)

iii. *Final Round*: Execute the following operations which are described above.

1. Sub Bytes
2. Shift Rows
3. Add Round Key, using

iv. *Encryption:* Each round consists of the following four steps:

1. Sub Bytes: The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.
2. Shift Rows : In the encryption, the transformation is called Shift Rows.

3. Mix Columns: The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.
4. Add Round Key: Add Round Key precedes one column at a time. Add RoundKey adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition. The last step consists of XORing the output of the previous three steps with four words from the key schedule. And the last round for encryption does not involve the "Mix columns" step.
5. Decryption: Decryption involves reversing all the steps taken in encryption using inverse functions like a) Inverse shift rows, b) Inverse substitute bytes, c) Add round key, and d) Inverse mix columns.

   The third step consists of XORing the output of the previous two steps with four words from the key schedule. And the last round for decryption does not involve the "Inverse mix columns" step.

b) Data Encryption Standard (DES)

DES (Data Encryption Standard) algorithm purpose is to provide a standard method for protecting sensitive commercial and unclassified data. In this same key used for encryption and decryption process.

DES algorithm consists of the following steps
Encryption

1) DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block.
2) The plaintext block has to shift the bits around.
3) The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
4) The plaintext and key will processed by following steps:
   i. The key is split into two 28 halves
   ii. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
   iii. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.
   iv. The rotated key halves from step 2 are used in next round.
   v. The data block is split into two 32-bit halves.
   vi. One half is subject to an expansion permutation to increase its size to 48 bits.
   vii. Output of step 6 is exclusive-OR'ed with the 48-bits compressed key from step 3.
   viii. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
   ix. Output of step 8 is subject to a P-box to permute the bits.
   x. The output from the P-box is exclusive-OR'ed with other half of the data block. k. The two data halves are swapped and become the next round's input.

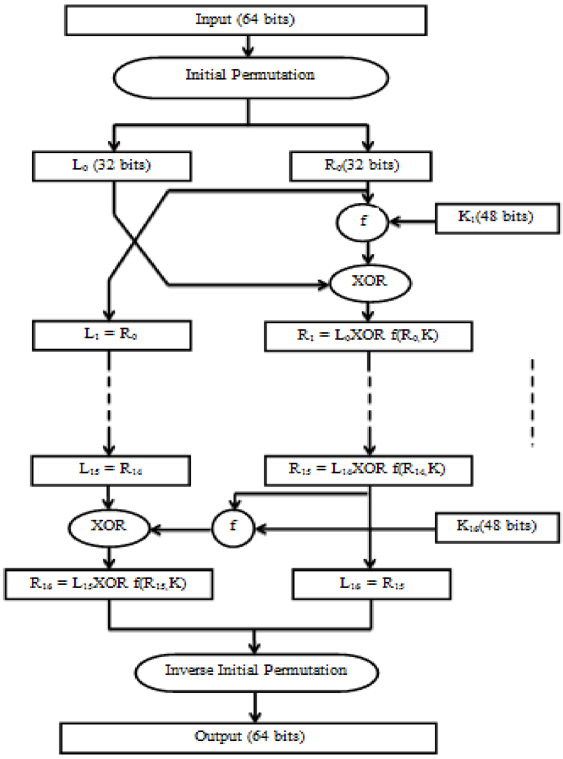


Figure 7: DES algorithm

DES algorithms purpose is to provide a standard method for protecting sensitive commercial and unclassified data. DES has small key size of 56 bits. It suffers from the problem of simple relation in keys. It is also susceptible to linear cryptanalysis attacks.

2) Asymmetric key algorithm:

a) Rivest-Shamir Adlemen(RSA)

RSA is widely used Public-Key algorithm. RSA firstly described in 1977. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it.

RSA algorithm involves these steps:

a) Key Generation
b) Encryption
c) Decryption

i.Key Generation: Before the data is encrypted, Key generation should be done.
Steps:
Generate a public/private key pair:
1. Generate two large distinct primes' p and q
2. Compute n = p*q and φ= (p − 1)(q − 1)
3. Select an e, 1 < e <φ, relatively prime to φ.
4. Compute the unique integer d, 1 < d <$\varphi$where e≡φ1.
5. Return public key (n, e) and private key d

ii. *Encryption:* Encryption is the process of converting original plain text (data) into cipher text (data).
Encryption with key (n, e)
1. Represent the message as an integer m € {0,.., n− 1}
2. Compute c = me mod n

iii *Decryption:* Decryption is the process of converting the cipher text (data) to the original plain text(data).
Decryption with key d: compute m = cd mod n.

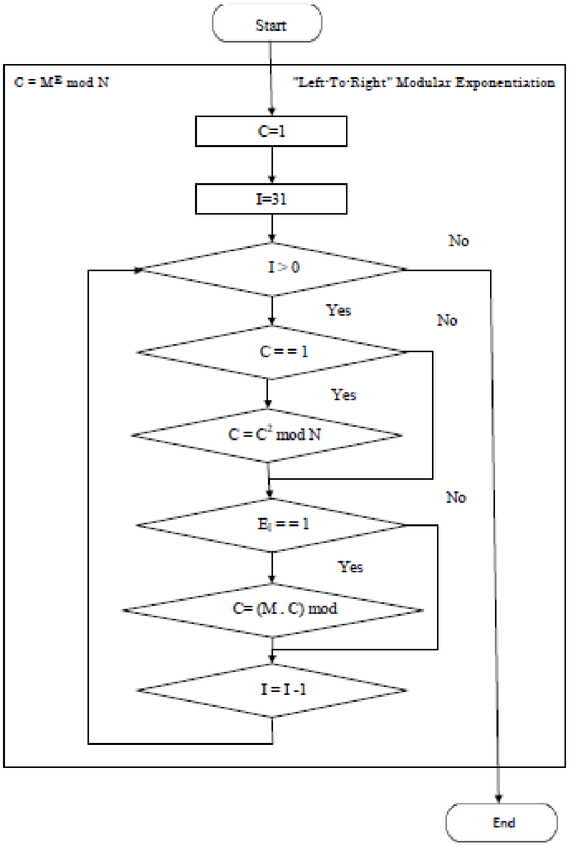


Figure 8: RSA algorithm

RSA uses larger integer 1024 bits for key size 2048 bits allow security for decade.

Surveyed Results And Analysis

According to paper “A Study of Encryption Algorithms AES, DES and RSA for Security” by Dr. Prerna Mahajan and Abhishek Sachdeva.

The four text files of different sizes are used to conduct four experiments, where a comparison of three.

Algorithms AES, DES and RSA is performed. Performance of encryption algorithm is evaluated considering the following parameters.
A. Encryption Time
B. Decryption Time

The encryption time is the time that an encryption algorithm takes to produces a cipher text from a plain text. Encryption time is used to calculate the throughput of an encryption scheme, is calculated as the total plaintext in bytes encrypted divided by the encryption time. Comparisons analyses of the results of the selected different encryption scheme are performed.

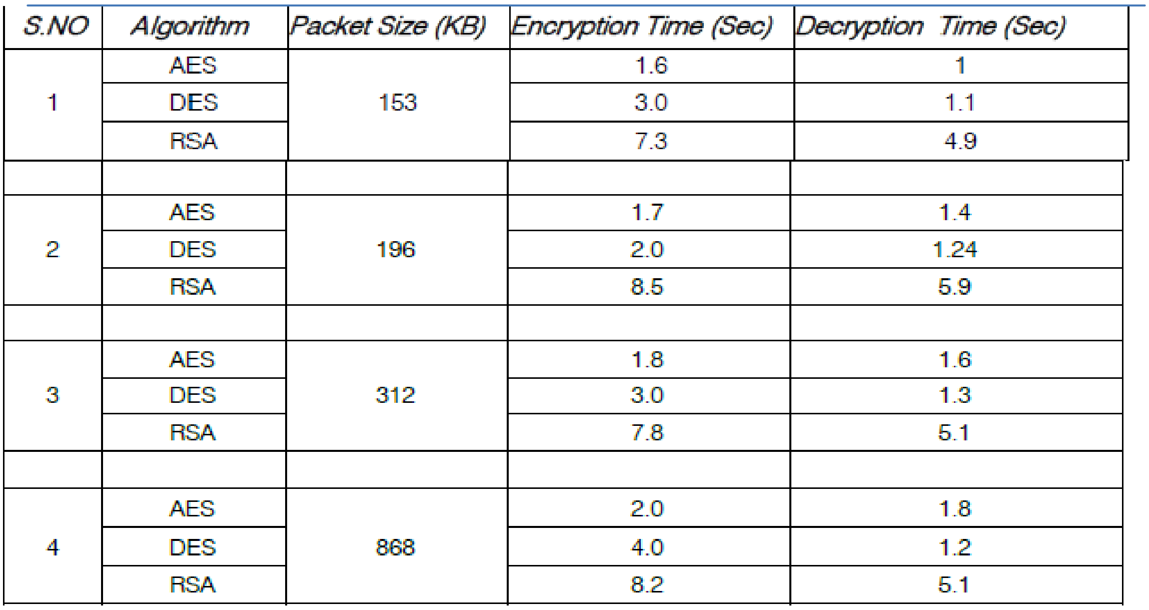
Experimental results for encryption algorithms

AES, DES and RSA are shown in fig 8, which shows the comparison of three algorithm AES, DES and RSA using same text file for four experiments.

Following table has experimented results.

6. Conclusion

Encryption technique plays very crucial role in world of networking security. Our paper surveyed the existing techniques like AES, DES, RSA algorithms based on their characteristics and performance. It has concluded that AES algorithm consumes least encryption time whereas RSA consumes longest encryption time but it has strong security. we also concluded that Decryption of AES is much better than other experimented algorithms. To get strong technique merits of AES and RSA can be integrated. Speed of AES and security of RSA can result into effective algorithm for encryption in a way to provide security to communication in network.



S.NO	Algorithm	Packet Size (KB)	Encryption Time (Sec)	Decryption Time (Sec)
1	AES	153	1.6	1
	DES		3.0	1.1
	RSA		7.3	4.9
2	AES	196	1.7	1.4
	DES		2.0	1.24
	RSA		8.5	5.9
3	AES	312	1.8	1.6
	DES		3.0	1.3
	RSA		7.8	5.1
4	AES	868	2.0	1.8
	DES		4.0	1.2
	RSA		8.2	5.1

Figure 9: comparison of AES, DES, RSA of encryption and decryption time

References

[1] [1] Anal Patel, Nimisha Patel, Rajan Patel "*Defending Against Wormhole Attack in MANET"*2015 Fifth International Conference on Communication Systems and Network Technologies

[2] BassantSelim, Chan YeobYeun, *"Key Management for the MANET: A Survey"* in 2015international conference on information and communication technology research.

[3] Praveen lalwaniDr. Sanjay SilakariPiyush Ku Shukla*"Optimized and Executive Survey On Mobile Ad-hoc Network"* In 2012 International Symposium on Cloud and Services Computing

[4] HumairaEhsan, FarrukhAslamKhan, "*MaliciousAODVImplementation and Analysis of Routing Attacks in MANETs*"in 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[5] Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala "*DoS Attacks in Mobile Ad-hoc Networks: A Survey"* in

[6] ond International Conference on Advanced Computing & Communication Technologies.

[7] Suresh Kumar GauravPruthiAshwaniYadavMukeshSingla "*Security protocols in MANETs*" in 2012 Second International Conference on Advanced Computing & Communication Technologies.

[8] PreetiNagrath, Bhawna Gupta "Wormhole Attacks in Wireless Adhoc Networks and their Counter Measurements:A Survey"

[9] Shushan Zhao, AkshaiAggarwal, Richard Frost, XiaoleBai "*A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks*" in IEEE communications surveys & tutorials, vol. 14, NO. 2, second quarter 2012

[10] Rakesh Kumar Jha, Suresh V. Limkar, Dr.Upena D. Dalal "A Performance Comparison of Routing Protocols for Security Issue In Wireless Mobile Ad Hoc Networks" in Third International Conference on Emerging Trends in Engineering and Technology

[11] LoayAbusalah, AshfaqKhokhar, and Mohsen Guizani*"A Survey of Secure Mobile Ad Hoc Routing Protocols*" in IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 10, NO. 4, FOURTH QUARTER 2008

[12] Kartik Kumar Srivastava, AvinashTripathi, Anjnesh Kumar Tiwari "*Secure Data Transmission In AODV Routing Protocol*" in International Journal of Communication and Computer Technologies Volume 01 – No.18, Issue: 04 April 2013

[13] M.Vijay, R.Sujatha "*Intrusion Detection System to Detect Malicious Misbehaviour Nodes in MANET*" in International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, March 2014

[14] Rakesh Kumar ER " *Applying Symmetric Key Cryptography for Security Issues in MANET's*" in Journal of Emerging Technologies and Innovative Research (JETIR) March 2015, Volume 2, Issue 3

[15] Dr.PrernaMahajan&AbhishekSachdeva "*A Study of Encryption Algorithms AES, DES and RSA forSecurity"* in Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013

[16] Rashmi, Dr. R Kanagavalli "*Utilization of Energy from Attacks Using RSA Algorithm in Wireless Ad hoc Sensor Network"* in International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 4, April 2015

[17] Prasad P. Lokulwar, Prof. YogadharPandey "*A Survey paper on Secure AODV protocol in MANAET using RSA algorithm and Diffie-hellman algorithm*" in International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013

[18] Miss.Rashmi P. Shinde, Mr. Sanjay S. Pawar*"SECURITY PROVIDED TO MOBILE AD-HOC NETWORKUSING RSA –ASYMMETRIC KEY CRYPTOGRAPHY"* in INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

[19] Mohamedi M. Mjahidi "*A Survey on Security Solutions of AODV Routing Protocol against Black Hole Attack in MANET "* in International Journal of Computer Applications (0975 – 8887) Volume 113 – No. 15, March 2015

[20] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi "*A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)*" in International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013