Comparative Analysis of Different Encryption Techniques in Mobile Ad-Hoc Networks (MANETs)

Apoorva Sharma[1], Gitika Kushwaha[2]

[1,2]Research Scholar, Institute of Information Technology & Management, New Delhi, India

apoorva.sharma098@gmail.com, gitika1512@gmail.com

***Abstract* -** This paper is in depth analysis of Data Encryption Standard (DES), Triple DES (3DES) and Advanced Encryption Standard (AES) even secret writing algorithms in painter was done victimization the Network Simulator 2(NS-2) in terms of energy consumption, information transfer time, End-to-End delay time and out turn with varied information sizes. 2 simulation models were adopted: the primary simulates the network performance assumptive the supply of the common key, and also the second simulates the network performance as well as the employment of the Diffie-Hellman Key Exchange (DHKE) protocol within the key management part. The obtained simulation results showed the prevalence of AES over DES by sixty fifth, seventieth and eighty three in term of the energy consumption, information transfer time, and network out turn severally. On the opposite hand, the results showed that AES is healthier than 3DES by around ninetieth for all of the performance metrics. Supported these results the AES was the suggested secret writing theme

***Keywords* -** *MANET, AES, DES, Key management.*

I. INTRODUCTION

In recent years, MANETs emerged as a serious next generation wireless networking technology. However, the safety problems on Manet became one amongst the first issues. MANETs square measure liable to attacks over wired networks. As a result, attacks with malicious goals can invariably devise to use these vulnerabilities and to disrupt the Edouard Manet operation. The matter display by potential breaching of the systems by passive observations and masquerading is more sophisticated by the variable nature of the wireless atmosphere [1].

Security is provided through security services like confidentiality. The goal of confidentiality is to manage or prohibit access to sensitive data to the sole approved people. Edouard Manet uses associate degree open medium, therefore sometimes all nodes among the transmission vary will acquire the information. a way to stay data confidential is to also be a threat to confidentiality if the scientific discipline keys aren't encrypted and hold on within the node [2].

Another challenge once it involves Edouard Manet security is that the key management issue. so as to stop the malicious nodes from connection within the networks, it is necessary to evidence the nodes once they square measure connection in Because of the restricted energy and machine capability of MANETs, it is necessary to style a light-weight weight and storage economical key management theme [3] [4].

Numerous security solutions, key management and scientific discipline techniques are designed to support Manet, a number of them square measure custom-made to suit the network necessities (minimum delay, minimum power

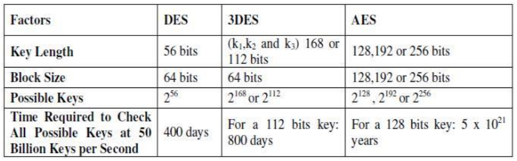
Consumption and most throughput) whereas others square measure famed to be computationally stern. They consume a substantial quantity of computing resources like information measure and power [5].

There is not any enough data regarding the potency of incorporating totally different coding techniques in unplanned networks.

This study was done to investigate DES, 3DES and AES coding techniques potency and suitableness for MANETs.

Table 1 shows a comparison between these coding techniques in line with [6].

Table 1. Comparison between DES, 3DES and AES



Factors	DES	3DES	AES
Key Length	56 bits	(k_1,k_2 and k_3) 168 or 112 bits	128,192 or 256 bits
Block Size	64 bits	64 bits	128,192 or 256 bits
Possible Keys	2^{56}	2^{168} or 2^{112}	2^{128} , 2^{192} or 2^{256}
Time Required to Check All Possible Keys at 50 Billion Keys per Second	400 days	For a 112 bits key: 800 days	For a 128 bits key: 5 x 10^{21} years

DH algorithmic rule was the primary revealed public key algorithmic rule by Diffie, and is generally spoken as DHKE. Several industrial products use this key exchange technique [7]. The purpose of the algorithmic rule is to permit 2 users to firmly exchange a key that may then be used for encryption. The algorithmic rule itself is proscribed to the exchange of secret values. The DH algorithmic rule depends for its potency on the problem of computing separate logarithms. DHKE algorithmic rule general steps square measure shown in Figure 1.

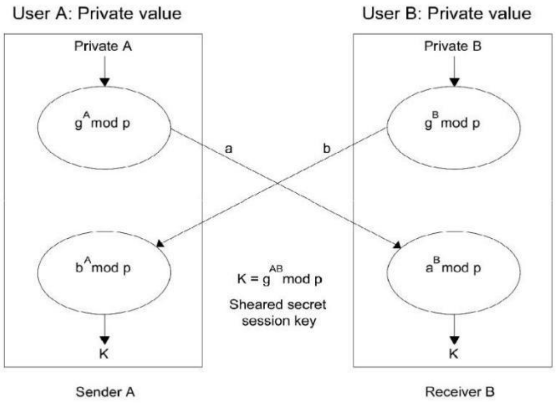


Figure 1. Diffie-Hellman Key Exchange Algorithm General Steps

The rest of this paper is organized as follows; section a pair of demonstrates the connected add the sphere of our study. Section three describes the implementation procedure of the cryptographic schemes in NS-2. Section four contains experimental results. Finally, this paper is complete in section five.

II. RELATED WORK

MANET security problems square measure quite common topic. we are going to survey some analysis efforts during this topic.

Some researchers targeted on the analysis of the performance of various coding schemes, others targeted on the key management and distribution problems that precede the particular encoding.

Mandal, et al.[8] projected a study that investigated the 2 most generally used symmetrical coding techniques DES and AES. The coding schemes had been enforced victimization MATrix

LABoratory (MATLAB) software package. once the implementation, these techniques were compared on some points, were theses points avalanched the result thanks to one bit variation in plain text keeping the key constant, avalanche result thanks to one bit variation in key keeping the plain text constant, memory needed for implementation and simulation time needed for coding. The authors finished that the DES coding algorithmic rule incorporates a disadvantage in term of high memory demand. Moreover, in AES the avalanche result is incredibly high in order that AES is good for encrypting messages sent between objects via unsecured channels, and is helpful for objects that square measure a part of financial transactions, and gave a future direction to incorporate experiments on alternative sorts of information like pictures.

Umaparvathi and Varughese in [9] bestowed a comparison of the foremost unremarkably used symmetrical coding algorithms AES (Rijndael), DES, 3DES and Blowfish in terms of power consumption. A comparison had been conducted for those coding algorithms victimization completely different information sorts like text, image, audio and video. The assorted coding algorithms had been enforced in Java. Within the experiments, the software package encrypts completely different file formats with file sizes (4MB - 11MB). The performance metrics like coding time, decipherment time and outturn had been collected. The bestowed simulation results showed that AES incorporates a higher performance than alternative common coding algorithms used. Since AES had not showed any celebrated security weak points within the bestowed study, this makes it a wonderful candidate. 3DES showed poor performance results sinceit needs additional process power. Since the battery power is one among the most important limitations in Manet nodes, the AES coding algorithmic rule is that the most suitable option.

Sahu and Kushwaha in [10] enforced symmetrical key coding algorithms DES, AES and Blowfish victimization NS-2 network machine to check their performance with completely different information sorts like text and image supported some performance metrics. within the experiments, the algorithms write a special file sorts like text, image and video sizes (0.3KB - 1KB). The performance metrics like coding and decipherment time, battery consumption, residual battery and outturn had been recorded for every file sort.

The projected symmetrical key coding algorithms were enforced victimization NS-2 (v-2.34) with completely different packet size, the gettable simulation results showed that AES is easy and higher in term of residual battery and coding time than alternative enforced algorithms. Blowfish had higher performance in term of outturn, however it consumes additional battery power compared with the opposite enforced algorithms.

Norouzi, et al. [11] targeted on the improvement of security performance associate degree exceedingly |in a wireless impromptu with an coding formula and transmission rate that planned. Simulation had been done victimisation MATLAB the input was text files with minimum size of fifty bytes and most size used is three hundred bytes,then these information transmitted victimization 2 modes; with coding and while not coding. For the primary mode, the information transmitted while not victimisation any coding. meantime for the second technique information transmitted with 3 coding algorithms; DES, AES and Blowfish. These algorithms were chosen as a result of they were usually employed in previous researches. throughout the conducted experiments only 1 key was accustomed inscribe and decipher information, that is that the largest size key within the specific formula.For the coding, information was encrypted with software system, Encrypt On Click for AES formula with 256 bit, Blowfish 2000 for Blowfish formula and Kryplite for DES formula. supported the input that is distance and size, time that Accustomed send information to receiver and turnout might be calculated. All of those calculation drained the MATLAB programming and also the output produces time of knowledge transfer. supported the gained results the authors suggested selecting AES to attain quick delivery of knowledge and high turnout, and selecting Blowfish formula once larger size of knowledge causation with smaller transmission rate.

Kashani and Mahriyar in [12] analyzed video streaming characteristics in impromptu networks victimisation many cryptography algorithms. The authors conferred associate degree application setup for secured video streaming in impromptu networks. Public key infrastructure approach was chosen to produce authentication at the network layer. They planned a completely distributed certification authority (CA) for Optimized Link State Routing (OLSR) primarily based impromptu networks. The initial assumption was that the network contains predefined special nodes known as shareholders. Shareholders will generate partial signatures. A node connection the network, will get a certificate given that it receives a minimum of k partial signatures type k completely different shareholders ,a investor providing service will be known from the broadcasted how-do-you-do messages.

On the opposite hand, completely different cryptography schemes were enforced and analyzed within the study; RC4, 3DES, AES-128, AES-256, Salsa20-128 and Salsa20-256 and also the time needed to inscribe completely different sizes of knowledge were adopted as a performance metric. The results showed that for RC4, 3DES, AES-128, AES-256, Salsa20-128 and Salsa20-256 took but one500 ms to inscribe the 1

MB computer file. 3DES consumes the biggest coding time followed by Salsa20-256, Salsa20-128, AES-256, AES-128 and RC4 severally.

Sandhiya, et al. [13] planned associate degree intrusion detection system named Enhanced Adaptive ACKnowledgment (EAACK) that consists of 3 parts; ACK, Secure ACKnowledgment (S-ACK), and misdeed Report

Authentication (MRA). All the acknowledgement packets were signed and verified to forestall cast acknowledgement packets. For linguistic communication and corroborative the acknowledgement packets, keys were generated and distributed earlier. The planned system uses one-hop ACK that accustomed enhance the misdeed of detection rates.

To eliminate the need of pre-distributed keys the planned system thought-about DHKE that depends on the problem of computing separate logarithms and permits user to firmly inscribe messages. NS-2 machine tool was used for running simulation, and also the results showed the advance of misdeed detection rates which ends up in lower routing overhead than the prevailing Intrusion Detection Systems (IDS) once victimisation the DHKE

Mechanism.

Du and Xiong in [3] planned a hop-by-hop authentication and routing driven dynamic key management them enamed HARD-KM. associate degree improved Elliptic Curve Diffie-Hellman (ECDH) protocol with mutual authentication was accustomed generate 2 combine keys, that were keep in caches before their expiration.

HARD-KM handling all nodes within the network equally rather than putt some cluster heads or a base station within the network, the theme used associate degree off-line certificate authority (CA) to sign certificates and distributed authentication materials matrix for all the mobile nodes.NS2 to machine was accustomed valuate HARD-KM feasibleness and potency.

The results showed that HARD-KM key management theme was resilient to the adversaries and reduces key cupboard space. The benefits of the planned key management theme were; neighboring pair-wise keys on demand creation to save lots of cupboard space, the pair-wise keys were derived from associate degree authentication materials matrix to wear down eavesdropping attack and compromised nodes had restricted threats to different uncompromised nodes.

Taneja, et al. [14] planned a standard secret key institution for even coding over impromptu networks victim misation DH key agreement protocol. The idea will be accustomed develop a brand new routing protocol for MANETs to produce most security against every kind of attacks. whereas DH key agreement protocol uses regular system to inscribe the information associate degreed an uneven system to inscribe the symmetric keys, the authors planned a protocol consists of 5 stages; the key generation and an exchange, shared secret creation, encrypting victimisation even key and encrypted information transmission.

CrypTool machine had been employed in modeling associate degreed testing the DH key agreement protocol that is an open supply e-learning application, employed in the implementation and analysis of cryptological algorithms. As a primary step in simulation, public parameters should be set. Since the general public parameters were freely accessible to any or all and thus, not solely supply and destination area unit ready to access these parameters rather each third party can also observe a similar. Once the general public parameters set, secret numbers of the supply and also the destination area unit chosen by pushing the button select secrets in CrypTool. Then the supply sends the shared key to the destination and contrariwise. As a final step, the supply and destination produce common and secret session key by pushing the button generates common session key in CrypTool. The implementation of a brand new security extension and cryptanalytic schemes square measure written as a brand new implementation within the NS-2[15].

This section discusses the new security agent and functions that been wont to simulate the performance of the encoding schemes of our interest. The NS-2 could be a common separate event machine developed chiefly for networking analysis. NS-2 is Associate in Nursing open supply software package provides wide simulating network sorts, network applications, routing protocols, information sources and network components. In NS-2, the system is sculptured as ordered events that take Associate in nursing discretionary quantity of your time. NS-2 is meant having 2 basic building blocks; C++ for the core practicality that handle processing and therefore the Object TCL (OTCL) for scripting functions that is just a special purpose language used for writing management script to run the simulation.

III. IMPLEMENTATION OF THE CRYPTOGRAPHIC SCHEMES IN NS-2

The protocol implementation needs the C++ language for packet process. and therefore the use of script language makes the modification of simulation configuration quicker and freely adjustable with dynamic parameters [15].

NS-2 is additionally supported with the Network AniMator (NAM) that offers a GUI of the network that's simulated. For MANET, NS-2 provides an oversized library for circumstantial routing, topology generators, propagation models, quality models and information sources. To run any simulation situation in NS-2, it should be written exploitation TCL script within the OTCL file [15]. though NS-2 offers various style alternatives it doesn't provide all. Our enforced cryptanalytic schemes and security extensions wasn't enclosed within the original NS-2, we've got enforced our supply codes and compiled viable files and record results supported some network metrics [15].

The security agent file throughout the protection institution method must be feed with the encoding kind from the supply and destination nodes through the TCL file. The encoding kind received from the TCL file hooked up with the encoding kind variable kind exploitation the bind statement. once a node receives the encoding kind and

therefore the key worth the particular encoding start by reading an information file with variable size exploitation the subsequent pseudo code:

```
Get pointer to file ("test.txt");
if (not permitted access file)
return (error);
read data items from ("test.txt");
read data as a separate block test
for end of file:
if yes end with read data;
return (done);
```

IV. SIMULATION AND RESULTS DISCUSSION

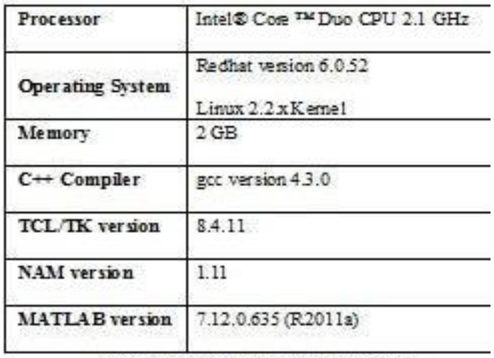
The two main functions of the enforced secret writing schemes performance analysis we have a tendency to had exhausted the unplanned network were; to perform a short study of the enforced symmetric performance, and to see the overhead that the DH formula adds to the general network performance.

During this Chapter we are going to gift the simulation results that we have a tendency to had recorded consistent with completely different performance metrics.

By considering completely different sizes of knowledge files (2 kilobyte to 64KB) the DES, 3DES and AES (128 key) secret writing algorithms were evaluated in terms of the energy consumption, knowledge transfer time and network output. All the implementations were balanced to form certain that the results are comparatively truthful and correct. The Simulation program accepts four inputs: the secret writing formula, secret writing mode, key and an computer file .once a winning execution, the cipher text generated.

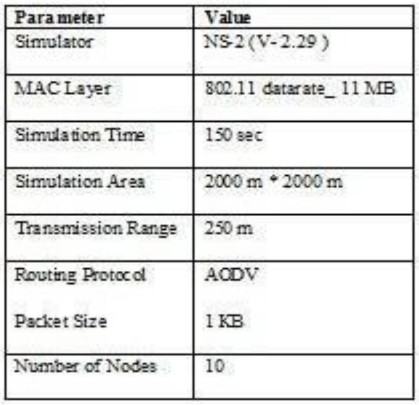
A. Simulation Parameters

Along with usual configuration of the wireless network simulation in NS-2, we have a tendency to had set the routing protocol as AODV mistreatment the command, set val(rp) AODV the macintosh layer, data rate, transmission vary, simulation space, simulation time, range of nodes and alternative details conjointly set within the network configuration TCL file. we have a tendency to used the AODV routing protocol for power optimisation, as a result of it needs less management packets. the main points of the pc system that we've got wont to compile NS-2 and run the simulation ar given in Table a pair of, and therefore the NS-2 simulation parameters that we have a tendency to utilized in our experiments as shown in Table 3. Table 3



Processor	Intel® Core ™ Duo CPU 2.1 GHz
Operating System	Redhat version 6.0.52 Linux 2.2.x Kernel
Memory	2 GB
C++ Compiler	gcc version 4.3.0
TCL/TK version	8.4.11
NAM version	1.11
MATLAB version	7.12.0.635 (R2011a)

Table 3. Simulation Parameters in NS-2



Parameter	**Value**
Simulator	NS-2 (V- 2.29)
MAC Layer	802.11 datarate_ 11 MB
Simulation Time	150 sec
Simulation Area	2000 m * 2000 m
Transmission Range	250 m
Routing Protocol Packet Size	AODV 1 KB
Number of Nodes	10

B. Simulation Factors and Metrics

The performance of enforced cryptanalytic schemes within the spontaneous network depends upon many factors:

1. Encryption schemes: This study evaluates 3 completely different symmetric algorithms; DES, AES (128 key) and 3DES.

2. Number of hops: within the conducted experiments the performance of the enforced cryptanalytic schemes was evaluated individually upon 3 main scenarios; one hop, 2 hops and 3 hops between the supply and therefore the destination nodes.

3.Data file size: the enforced algorithms encipher completely different file sizes; 2KB, 4KB, 8KB, 16KB, 32KB and 64KB.

4. Simulation models: In our study we have a tendency to applied 2 simulation modes; the primary mode simulates the network behavior forward the supply of the common key, and therefore the second mode simulates the network behavior as well as the key management innovate the link sensing between the supply and therefore the destination nodes to confirm areliable and secure key management that precedes the particular coding.

We have performed many tests on our enforced cryptanalytic schemes to watch its performance exploitation many performance metrics that area unit outlined in Table 4

Table 4. Simulation Metrics

Metric	Definition
The energy Consumption (Joule)	The energy consumption is the average amount of energy consumed by th encryption and decryption during algorithm processing.
The data transfer time (sec)	The time from starting the encryption of the first packet in a selected data file till the end of the decryption of the last encrypted packet that reached the destination node including the End-to-End delay time.
End-to-End delay time (sec).	The time taken for a packet to be transmitted across a network from source to destination.
The network Throughput (Kb/sec)	The network throughput that evaluated by dividing the total plaintext size that been encrypted on the total encryption time consumed during encryption.

Performance analysis assumptions:

1. Free house network with no multipath and/or attenuation
2. No noise touching the network
3. 20 repetitions for every experiment.

Results and Discussion

This Section discusses the performance supported the chosen metrics upon the variable factors that elaborated within the previous section.

1) Energy Consumption

In our experiments the energy consumption was evaluated exploitation constant technique delineated in [16]. we tend to gift a basic value of secret writing and decoding conferred by the merchandise of the whole range of clock cycles taken by the secret writing and also the average current drawn by every CPU clock cycle. The author in [17] showed the price of some secret writing algorithms on Pentium processor as clock cycles per computer memory unit, that we tend to employed in our calculations as shown in Table 4. To calculate the whole energy value, we tend to divide the price in Amperes for all secret writing and decoding clock cycles by the processor clock speed in cycles/sec.

For a Pentium processor the clock speed is 7590 cycle/sec as shown in [18] that employed in our calculations as shown in Table 4. The energy value calculations per computer memory unit done exploitation the subsequent equation, and also the Energy consumption for various file sizes area unit shown in figure 2 for DES, 3DES and AES secret writing schemes.

Table 2. System Configuration

Processor	Intel® Core ™ Duo CPU 2.1 GHz
Operating System	Redhat version 6.0.52 Linux 2.2.x Kernel
Memory	2 GB
C++ Compiler	gcc version 4.3.0
TCL/TK version	8.4.11
NAM version	1.11
MATLAB version	7.12.0.635 (R2011a)

Table 3. Simulation Parameters in NS-2

Parameter	Value
Simulator	NS-2 (V- 2.29)
MAC Layer	802.11 datarate_ 11 MB
Simulation Time	150 sec
Simulation Area	2000 m * 2000 m
Transmission Range	250 m
Routing Protocol	AODV
Packet Size	1 KB
Number of Nodes	10

$$E = \frac{(CC/B)}{CS} * I * V$$

Table 5. Energy Consumption Results

Algorithm	Clock Cycles/B	Energy (mJoule)
DES	90	117.4
AES	32	42
3DES	216	280

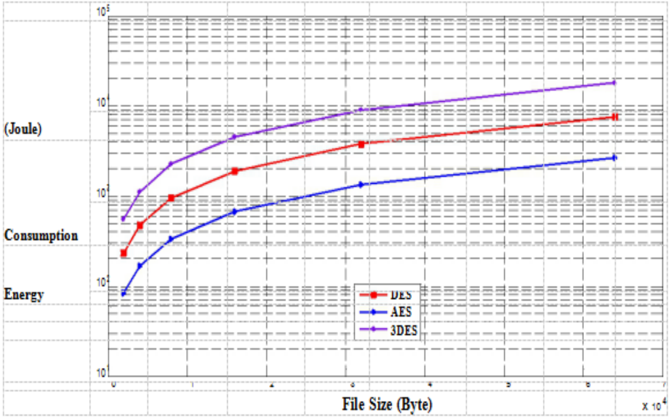


Figure 2: Energy Consumption for Varying Data File Sizes

In general the results showed the prevalence of AES rule over DES and 3DES in term of the energy consumption

(when inscribe identical knowledge file).

Actually, we tend to found that the AES needs around sixty fifth, eighty fifth energy less that the energy consumed by DES and 3DES algorithms severally.

DES rule consumes around fifty eight energy but 3DES rule.

2) Data Transfer Time

The data transfer time calculations in our conducted experiments were supported an equivalent technique utilized by[11] that thought-about because the time from beginning the secret writing of the primary packet in an exceedingly hand-picked record until the tip of the cryptography of the last encrypted packet that reached the destination node together with the End-to-End delay time. so as to work out the transfer time the subsequent equation was used:

$$T_r = T_e + T_d + T_{EE}$$

$$T_e \cong T_d \cong \sum_1^{N_p} T_i$$

$$N_p = F_s / P_s$$

For the implemented encryption schemes in our study the transfer time results are shown graphically in Figure. 3.

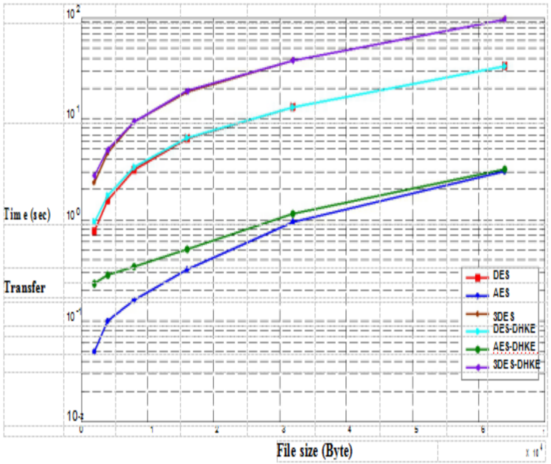


Fig.3 : The Implemented Encryption Schemes Transfer Time Results for the Two Simulation Modes

As we will notice from Figure 4 a bonus of victimization the AES secret writing theme is that it takes less information transfer time than DES and 3DES secret writing schemes. The experimental results showed that the AES transfer time is some ninetieth but DES secret writing once running simulation mode one. On the opposite hand, AES consumes associate degree some twenty fifth transfer time but DES secret writing for tiny information files and (57%-80%) but DES for larger information files once applying the DHKE rule in simulation mode 2 applied experiments (loading constant information sizes for each secret writing schemes).

3) Network Throughput

In our study the throughput of the network whereas running the enforced coding schemes is calculated exploitation the formula given by [11], that done by normalizing the whole encrypted file size in bytes by the information transfer time exploitation the subsequent formula:

Throughput = size of plain text / time consumed during encryption

For different record sizes the throughput results whereas running the 2 simulation modes area unit shown in Figure 4.

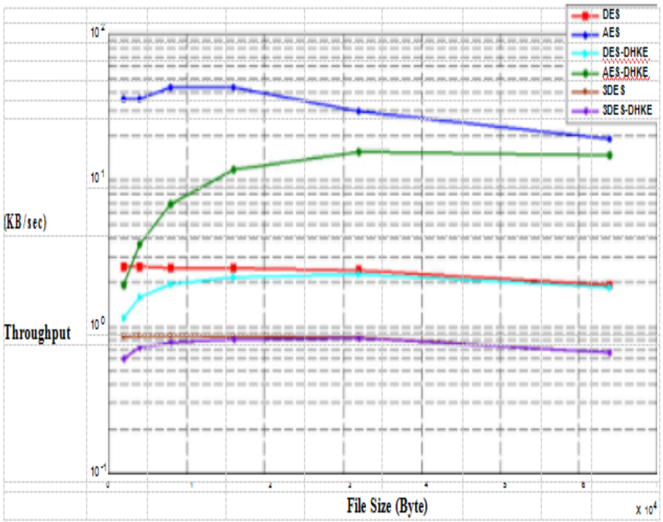


Fig.4: Network Throughput Results for the Implemented Encryption Schemes End-to-End Delay Time

The End-to-End delay time in our study measured because the measure from the instant that the supply node sends a primary packet of information once secret writing procedure completion till the instant that the destination node within the network receives the last encrypted packet. in keeping with the End-to-End delay definition the DHKE transactions adds a definite preprocessing time overhead to the particular End-to-End delay time between supply and destination nodes now is fastened for DES, 3DES and AES as a result of it's associated with the transfer packets throughout session initiation stage and not the particular encoding. forward totally different variety of hops between the supply and destination nodes, and exploitation 16KB record size the End-to-End delay time results square measure shown in "Fig. 5" for the 2 applied simulation modes. usually the file size VS. the proportion of the DHKE overhead is shown in Table 6.

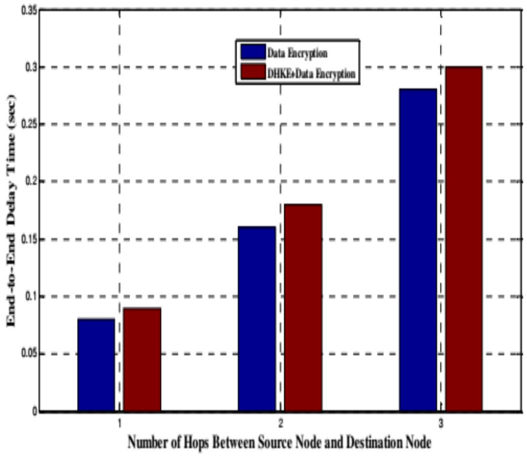


Figure 5 Ad hoc Network End-to-End Delay Time Calculations for 16KB Data

Table 6 The Data File Size VS. DHKE Overhead

The following conclusions were obtained:

File Size (KB)	DHKE Overhead (%)
1	66.7
2	50
4	33.3
8	20
16	11.1

From the results shown within the on top of table we will conclude that the overhead caused by applying DHKE protocol to the general Manet performance is suitable scrutiny with its edges particularly for giant information files.

V. CONCLUSIONS AND FUTURE DIRECTIONS

In this study we have a tendency to tried to judge the performance of DES, 3DES and AES bilateral coding algorithms beneath painter setting. On the opposite hand, we have a tendency to applied a secure key management resolution exploitation the DHKE protocol. and eventually we have a tendency to offered the power to decide on the coding sort by the user supported the specified security level.

Table 7. Performance Evaluation Results Summary

Performance	**AES superiority over**	**AES superiority over**	**DES superiority over**
Metric	DES (%)	3DES (%)	3DES (%)
Energy	65	85	59
Consumption			
Transfer Time	70	95	63
Network	83	95	64
Throughput			

Security in unintentional networks is associate degree open analysis issue, and fact-finding work remains in progress for brand spanking new security solutions. The scientific discipline solutions, and their suitableness with unintentional limitations, can perpetually be a challenge so as to produce protection from malicious attacks. The followings ar some future work suggestions:

•Analyze and measure the performance of another isobilateral block cipher like the Blowfish cipher.

•Analyze and measure the performance of stream cipher cryptography like the RC4 and SEAL ciphers. A comparative analysis of stream cipher cryptography with block cipher cryptography is assumed to be valuable.

•Evaluate the performance of the network victimisation another network machine like Opnet network machine so as to validate the obtained thesis results.

•Evaluate the performance of the network with totally different network topologies.

•Evaluate the performance of the network forward new nodes joining/leaving the network.

REFERENCES

[1] Nadeem, A. and Howarth, M. P. (2013), A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks. IEEE Communications Surveys & Tutorials, 15(4), 2027-2045.

[2] 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.

[3] Du, D. and Xiong, H. (2011), A Dynamic Key Management Scheme for MANETs. In Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), IEEE, 1, 779-783.

[4] Mokhtarnameh, R. Muthuvelu, N. Ho, S. B. and Chai, I. (2010), A Comparison Study on Key Exchange-Authentication Protocol. International Journal of Computer Applications IJCA, 7(5), 5-11.

[5] 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.

[6] Alanazi, H., Zaidan, B. B., Zaidan, A. A., Jalab, H. A., Shabbir, M. and Al-Nabhani, Y. (2010). New comparative study between DES, 3DES and AES within nine factors. arXiv preprint arXiv:1003.4085.

[7] Stallings, W. (2006), Cryptography and Network Security: Principles and Practice, (5^th ed.). India: Pearson Education.

[8] 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.

[9] 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.

[10] 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).

[11] Norouzi, M. esmaeel Akbari, M. and Souri, A. (2012), Optimization of Security Performance in MANET. Journal of American Science, 8(6).

[12] Kashani, A. A. and Mahriyar, H. (2014), A New Method for Securely Streaming Real-time Video in Ad hoc Networks. Advances in Environmental Biology, 8(10), 1331-1338.

[13] Sandhiya, D. Sangeetha, K. and Latha, R. S. (2014), Adaptive ACKnowledgement Technique with Key Exchange Mechanism for MANET. In Electronics and Communication Systems (ICECS), 2014 International Conference, IEEE, 1-5.

[14] Taneja, S. Kush, A. and Hwang, C. J. (2011), Secret Key Establishment for Symmetric Encryption over Adhoc Networks. In Proceedings of the World Congress on Engineering and Computer Science (Vol. 2).

[15] Fall, K. and Varadhan, K. (2002). The NS Manual. Notes and Documentation on the Software NS2-Simulator.

[16] 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.

[17] Biham, E. (Ed.). (2006), Fast Software Encryption. 4th International Workshop, FSE'97, Haifa, Israel, January 20-22, 1997, Springer, Proceedings (Vol. 1267).

[18] Rhett, (1999), x86 CPU Reference, Part 2. Retrieved May 25, 2015, from http://alasir.com/x86ref/index.htm