Optimization of Security Performance in MANET

Monire Norouzi[1], Mohammad esmaeel Akbari [2], Alireza Souri [3]

[1, 3] Department of Computer Engineering, Ahar Branch, Islamic Azad University, Ahar, Iran
[2]Department of Electrical Engineering, Ahar Branch, Islamic Azad University, Ahar, Iran
E-mail: m-norouzi@iau-Ahar.ac.ir, m-Akbari@iau-Ahar.ac.ir, a-souri@iau-Ahar.ac.ir

Abstract: Nowadays wireless technology is widely used in variety of handheld devices which required different security requirements. All this mobile computing devices enable to form mobile ad hoc network or MANET. To ensure all the transmission secured, we need suitable encryption algorithm. It can protect the confidentiality of data from malicious attack. Beside that it can be used as a mechanism to ensure that data were equipped with security features such as authentication, integrity and confidentiality. This paper will focus on the impact of performance security environment in an ad hoc wireless with a suitable encryption algorithm and transmission rate that has been determined. One simulation had been done using Matlab. Based on the result are showed that the data had been encrypted with AES algorithm gained smallest time transfer. AES produced high throughput with 50 bytes size when transmission rate is 11 Mbps and when both size and transmission increased. Meanwhile Blowfish algorithm produced high throughput in larger size when transmission rate is low. Besides that, throughput gave low impact to size in same transmission rate but high produces throughput when the value was increased.
[Monire Norouzi, Mohammad esmaeel Akbari, Alireza Souri. **Optimization of Security Performance in MANET.** *J Am Sci* 2012;8(6):779-784]. (ISSN: 1545-1003). http://www.americanscience.org. 98

Keywords: Computer Security; Ad-Hoc Wireless; Encryption Algorithm; Transmission Rate; throughput.

1. Introduction

Rapid changes in technology give an opportunity to users a variety of choices in communication channels. As we know, latest trends in this millennium had enforced users to accept and use current technology. One of these recent technologies is wireless communications which has been a part of facilities provided by owners of buildings. These wireless facilities are available in public places such as cafe, library, airport, hotels and also lobby of office buildings. This is to ensure that everybody is connected to the Internet through wireless devices. Today the way of communications are growing very fast which requires everyone to be connected and they wanted information to be at their fingertips. They want to access all these information quickly because as faster information retrieve it will be more valuable. Based on the human needs, the innovation of variety handheld devices such as smart phone, tablet computer and others devices had been created. These devices are supported by wireless technology. This new paradigm is known as mobile computing. [1] Mobile computing enables to form ad hoc wireless network. It is self organizing and adaptive which means it not rely on any fixed network entities. It can be heterogeneous such with mobile computing devices.

Commonly ad hoc network also known as mobile ad hoc network (MANET) [2] Nowadays mobile computing became necessity gadget to those who always busy working and moving around. Security of this devices should be a high priority and users themselves have to aware and well-versed with their own mobile devices to be secured and protect from malicious attacks.[3] MANET also cannot avoid the security problem that exists. The challenge security can due to unpredictable topology, wireless shared medium, heterogeneous resources and stringent resource constraints. [4] There are three security perspective challenges in mobile environment; User, Network and service provider [5]. Security is very important and should be major issues to consider by telecommunications provider, manufacturers and also to the end users. Variety of wireless devices had created different requirement to have secure connections. It arises from different hardware, software, wireless medium, system resources and also channels quality. As for the solution middleware known as AsecMid proposed .[6] It can dynamically select the protocol based on the wireless environments. The results showed stronger protocol will degrade the throughput based on the parameters and metric mentioned before. But the result does not depend on the transmission rate and the author also mentioned in their future works to make further study on that issue. The other study that related to transmission rate done by [7] discussed how to select the transmission rate to get maximum throughput. This transmission rate depends on the distance between two nodes. The research determined two types of transmission which is fixed transmission rate at each link and at each node. Their scheme tries to get maximum throughput with condition that connectivity wireless mesh network were kept. They

evaluate their scheme by using test bed and the result showed there was minimum improvement.

This study seems to be less efficient because of the length of time taken to run this experiment. Meanwhile some researchers relate it with algorithm that can balance the size of space known as distributed parameters-tuning algorithm (DPA). The proposed algorithm also can be implementing in most of 802.11 networks.[10]. Based on the result of simulation, DPA could balance the relationship between level of spatial reuse and transmission rate. Their method to set the value of transmission rate can be applied in the research that had been proposed.

A lot of research has been done to study about security issues in mobile computing, where some of them focused on their performance. Mostly the solution that suggested was involved with the middleware and some of them related with power consumption of the mobile devices. Meanwhile, there are other solutions such as proposed algorithm that can produce better throughput and it also will improve the performance of the mobile networks. A wide of research had been done to get best throughput based on transmission rate with another factor such as algorithm, power consumption and also use fix nodes. Most of them use a simulator and they also prove their solution through test bed. Based on the literature had been done, it showed that suitable transmission rate is important in order to achieve best throughput. Another factor should be considered is encryption algorithm used to ensure that data sent were secured. The purpose of this paper is to describe deployment issues in security of MANET that concerns about their encryption algorithm.

As for this study, it will produce time transfer based on the size data and the data that has been encrypt with selected encryption algorithm used. It will relate with the transmission rate that used and to see the impact to performance of the throughput. Based on the results of the experiments, it will give an option to the users to select the algorithm that can give better performance with suitable transmission rate. This paper is organized as follows. Firstly background of the mobile computing and their security will be presented in the introduction. Second part will describe the material and method used. Then it followed by findings produced. Lastly conclusion of the study will be presented.

Rapid changes in technology give an opportunity to users a variety of choices in communication channels. As we know, latest trends in this millennium had enforced users to accept and use current technology. One of these recent technologies is wireless communications which has been a part of facilities provided by owners of buildings. These wireless facilities are available in public places such as cafe, library, airport, hotels and also lobby of office buildings. This is to ensure that everybody is connected to the Internet through wireless devices. Today the way of communications are growing very fast which requires everyone to be connected and they wanted information to be at their fingertips. They want to access all these information quickly because as faster information retrieve it will be more valuable. Based on the human needs, the innovation of variety handheld devices such as smart phone, tablet computer and others devices had been created. These devices are supported by wireless technology. This new paradigm is known as mobile computing. [1] Mobile computing enables to form ad hoc wireless network. It is self organizing and adaptive which means it not rely on any fixed network entities. It can be heterogeneous such with mobile computing devices.

Commonly ad hoc network also known as mobile ad hoc network (MANET) [2] Nowadays mobile computing became necessity gadget to those who always busy working and moving around. Security of this devices should be a high priority and users themselves have to aware and well-versed with their own mobile devices to be secured and protect from malicious attacks.[3] MANET also cannot avoid the security problem that exists. The challenge security can due to unpredictable topology, wireless shared medium, heterogeneous resources and stringent resource constraints. [4] There are three security perspective challenges in mobile environment; User, Network and service provider [5]. Security is very important and should be major issues to consider by telecommunications provider, manufacturers and also to the end users. Variety of wireless devices had created different requirement to have secure connections. It arises from different hardware, software, wireless medium, system resources and also channels quality. As for the solution middleware known as AsecMid proposed .[6] It can dynamically select the protocol based on the wireless environments. The results showed stronger protocol will degrade the throughput based on the parameters and metric mentioned before. But the result does not depend on the transmission rate and the author also mentioned in their future works to make further study on that issue. The other study that related to transmission rate done by [7] discussed how to select the transmission rate to get maximum throughput. This transmission rate depends on the distance between two nodes. The research determined two types of transmission which is fixed transmission rate at each link and at each node. Their scheme tries to get maximum throughput with condition that connectivity wireless mesh network were kept. They

evaluate their scheme by using test bed and the result showed there was minimum improvement.

This study seems to be less efficient because of the length of time taken to run this experiment. Meanwhile some researchers relate it with algorithm that can balance the size of space known as distributed parameters-tuning algorithm (DPA). The proposed algorithm also can be implementing in most of 802.11 networks.[10]. Based on the result of simulation, DPA could balance the relationship between level of spatial reuse and transmission rate. Their method to set the value of transmission rate can be applied in the research that had been proposed.

A lot of research has been done to study about security issues in mobile computing, where some of them focused on their performance. Mostly the solution that suggested was involved with the middleware and some of them related with power consumption of the mobile devices. Meanwhile, there are other solutions such as proposed algorithm that can produce better throughput and it also will improve the performance of the mobile networks. A wide of research had been done to get best throughput based on transmission rate with another factor such as algorithm, power consumption and also use fix nodes. Most of them use a simulator and they also prove their solution through test bed. Based on the literature had been done, it showed that suitable transmission rate is important in order to achieve best throughput. Another factor should be considered is encryption algorithm used to ensure that data sent were secured. The purpose of this paper is to describe deployment issues in security of MANET that concerns about their encryption algorithm.

As for this study, it will produce time transfer based on the size data and the data that has been encrypt with selected encryption algorithm used. It will relate with the transmission rate that used and to see the impact to performance of the throughput. Based on the results of the experiments, it will give an option to the users to select the algorithm that can give better performance with suitable transmission rate. This paper is organized as follows. Firstly background of the mobile computing and their security will be presented in the introduction. Second part will describe the material and method used. Then it followed by findings produced. Lastly conclusion of the study will be presented.

2. Principles and Methods

The material for this research was based on the previous research from [8] about ideal transmission rate for ad hoc. As for this experiment it will involve with 2 nodes. For instance, the nodes location that might be involved can be illustrated as in Figure 1.

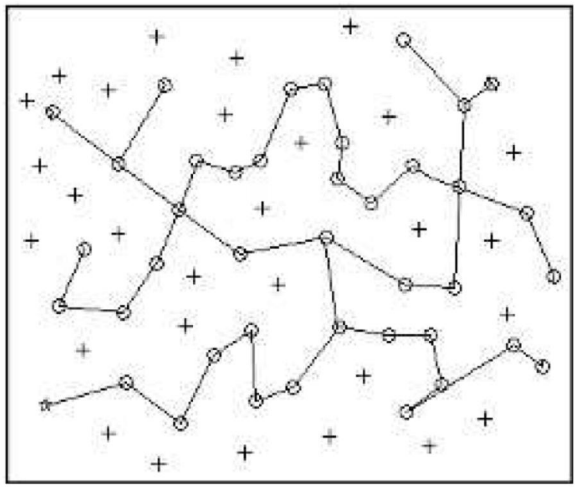

Figure:1 An example of network with nodes

The similar method was applied in [9], which is they used two notebooks to evaluate encryption algorithm on power consumption. The purpose of study is how the several encryption algorithms affect the consumption of battery power with and without data transmission. It showed that the same method can be applied for this experiment.

As for these studies, input for this programming was the distance of two nodes which could be 15m or 30m. . It can be identified by distance of the two nodes used such as transmission rate of 1 or 2 Mbps, 5.5 Mbps and 11Mbps are ideal distances of 100m,60m and 30m. For this experiment, the rate used is 11Mbps and 22Mbps with distance 30m and 15m respectively [10]. Meanwhile for the time for transfer rate for ad hoc it based on [11]. It was mentioned that transfer time for file sized of 10Mb was 90s. From here the time transferred for those file can be calculated and it done through written program using Matlab another input was the size of data in textfile with minimum size of 50 bytes and maximum size used is 300 bytes.

Then these data will be transmitted data using two modes; with encryption and without encryption. First data will be transmitted without using any encryption. Meanwhile for the second method it will transmit with data that have been encrypted. To ensure security of the data and its confidentiality, the data will be tested with three encryption algorithms such as: DES, AES and Blowfish.

These algorithms are chosen because it was a common algorithm used in previous research. Variations of this algorithm had been used in order to run in AsecMid middleware [12]. Six encryption algorithms include above algorithm also had been used in the test bed experiments, as mentioned in earlier paragraph. [13] As for the symmetric key used for these algorithms, only one key will be used to

encrypt and decrypt data, which is the largest size key in the particular algorithm.

Strength of symmetric key encryption depends on the size of the key used. [3] For the encryption, data was encrypted with freeware, EncryptOnClick for AES Algorithm with 256 bit, Blowfish 2000 for Blowfish algorithm and Kryplite for DES algorithm. Size of this data was an input for the programming. Based on the input which is distance and size, time that used to send data to receiver and throughput could be calculate. All of these calculation done in the Matlab programming and the output would produce time of data transfer. Based on size data used and time, formula for throughput can be calculated in the programming:

Throughput = size of plain text / time

3. Results

After the experiments done by using above method, it produced the results. It based on transmission rate, data without encryption, encrypted data, size of data, transfer time and lastly throughput of the network. The results were divided into two categories which is; data size that includes data without encryption and data that have been encrypt with the encryption algorithm. Beside that it also based on the transmission rate used.

As for the data used it has been transmit from sender to receiver, which is the size of data used is 50 bytes and 300 bytes. Meanwhile as the transmission rate was based from the ideal distance. The results produced as in the Table 1. It divided in three sections which are; size data, time transfer and lastly throughput. All these based on the data not being encrypted and also selected encryption algorithm.

For transmission rate 11 Mbps with ideal distance 30metres. The result shows that size is increase after encryption and for time transfer of data size 50 bytes became slower after encrypt with encryption algorithm and became slowest when it encrypt with DES algorithm. Meanwhile for throughput, the results show that, AES produce highest throughput among these three algorithms.

Table 1: DATASIZE 50 byte WITH 11 Mbps TRANSMISSION RATE

Type Data	Size (bytes)	Time (Sec)	Throughput
No encrypt	50	0.4394	113.7915
AES	299	2.6279	113.7791
blowfish	818	7.1894	113.7786
DES	1280	11.25	113.7778

From the table, the graph of the results can be shown as in the Figure 2.

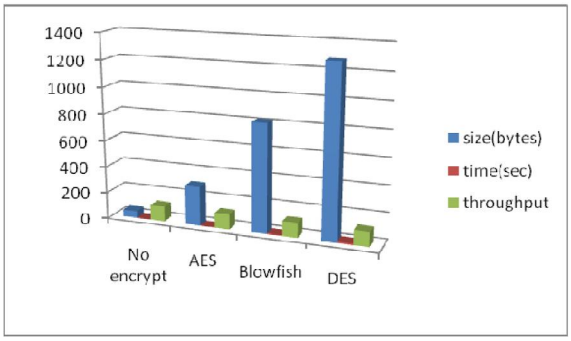

Figure:2 Result of data size 50 bytes with Transmission rate 11Mbps

As illustrated in the graph, the size increase after being encrypt with the algorithm and the Blowfish algorithm produce high throughput. Then the same data size with was encrypted with 22 Mbps transmission rate and the ideal distance is 15 meters. The same method used which data encrypted with AES,DES and Blowfish. It also used data that not being encrypted. This produced the results in table 2.

Table 2: DATASIZE 50 byte WITH 22 Mbps TRANSMISSION RATE

Type Data	Size (bytes)	Time (Sec)	Throughput
No encrypt	50	0.21973	227.5519
AES	299	1.3140	227.5494
blowfish	818	3.5947	227.5572
DES	1280	5.625	227.5555

The data shows that the time transfer was decrease from 11 Mbps to 22 Mbps when it encrypt with all the algorithm.. Meanwhile the time transferred it increased after the encryption process. This made throughput increased when the data was encrypted. When compared between three algorithms, it shows that Blowfish produced high throughput than DES and AES. All of these results can be shown in the graph Figure 3.

Then the experiment tested with the bigger size which is 300 bytes. The same process done as it the file encrypted with the encryption software that based on AES, DES and also Blowfish.

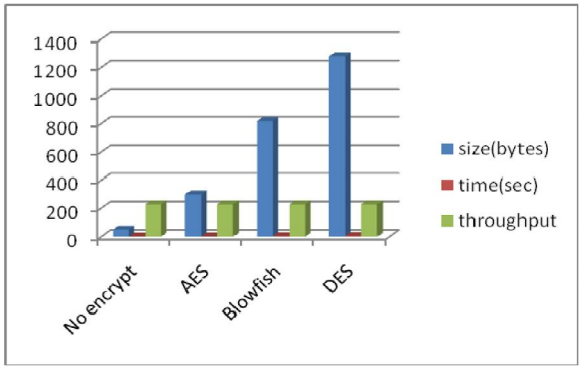

Figure 3. Result of data size 50 bytes with rate 22 Mbps

Table 3: DATASIZE 300 byte WITH 11 Mbps TRANSMISSION RATE

Type Data	Size (bytes)	Time (Sec)	Throughput
No encrypt	300	2.6367	113.7785
AES	415	3.6475	113.7765
blowfish	1065	9.3604	113.7771
DES	1361.9	11.97	113.7761

Based on the result, time transfer was increased when the transmission rate was decrease when data was encrypted. It leads to higher throughput if compared with different encryption algorithm where Blowfish show the highest throughput. From the results, graph was plotted based on the throughput produced for each data size and transmissions rate.

In Figure 4, it shows that data that have been encrypt with AES, Blowfish and DES encryption algorithm gave similar throughput and the difference is not really significant.

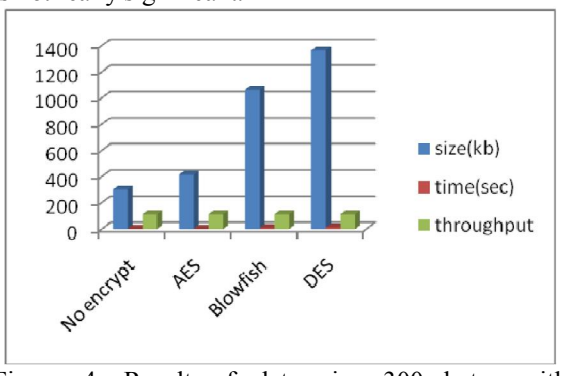

Figure 4. Result of data size 300 bytes with Transmission rate 11 Mbps

Then for the throughput with different rate but with same size is shown in the table and graph below:

Table 4: DATASIZE 300 byte WITH 22 Mbps TRANSMISSION RATE

Type Data	Size (bytes)	Time (Sec)	Throughput
No encrypt	300	1.3184	227.5485
AES	415	1.8237	227.5593
blowfish	1065	4.6802	227.5543
DES	1361.9	5.9849	227.5560

Based on the table 4, time for transfer data was faster than normal data compared encrypt data. If we compared between all algorithms, there is not really huge difference. These results also gave same impact in throughput. Then all this data have been plot in the graph as shown in Figure 5.0 with data size 300 bytes.

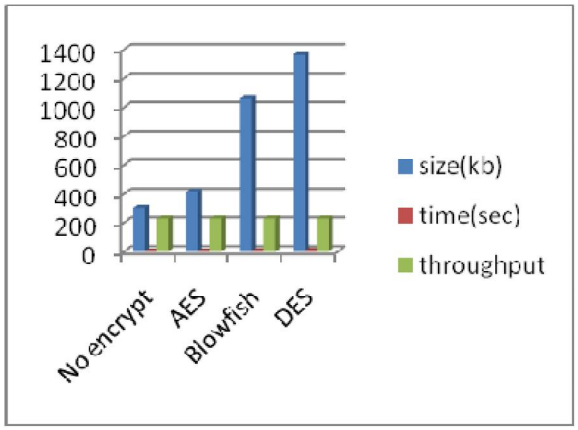

Figure 5. Result of data size 300 bytes with Transmission rate 22 Mbps

All of these outcomes as mentioned above were based on the data that were obtained from previous study that can be related with transmission rate and performance in ad hoc wireless.

4. Conclusion

Based on the results, the throughput of the transmission was higher if the transmission is increase. The selection of encryption algorithm will give an impact to the throughput, when minimum size which is 50 bytes size used with transmission rate 11 Mbps, AES algorithm produced higher throughput with size increased to 299 bytes. When transmission rate is higher, which is 22 Mbps, Blowfish algorithm gave higher throughput. If we use larger size, which is 300 bytes, Blowfish algorithm gave higher throughput in for 11Mbps transmission rate. Meanwhile when transmission rate was 22 Mbps,

AES algorithm produced highest throughput. In term of time transfer, AES produced fastest time in sending data for all transmission rates because of smaller size compared to other algorithm. Based on above results, to optimize performance in ad hoc wireless, users should choose AES to achieve fast for access data but have to choose Blowfish algorithm when they used larger size with smaller transmission rate. But for the short distance, with higher transmission rate, AES algorithm produced high throughput. Meanwhile for the smaller size to gain higher throughput, user should choose AES algorithm and used Blowfish when transmission rate is high. But any option of encryption algorithm used only gave small difference. As nowadays the usage of mobile are very wide and by using this method users can exchange or transfer file among each other without any worries of security issues.

Corresponding Author:
Monire Norouzi
Department of Computer Engineering,
Ahar Branch, Islamic Azad University,
Ahar, Iran
E-mail: m-norouzi@iau-Ahar.ac.ir

References

1. Yuan Zhang,"Programmable and Active Networks", Master Thesis,McGill University, Montreal. (1999).
2. C.K Toh, M. Delwar, D. Allen, "Evaluating the communication performance of an ad hoc wireless network", IEEE Transaction on wireless communications, 1(3); 402-414. (2002).
3. Botha RA, Furnell SM Clarke NL, "From desktop to mobile: examining the security experience". Computer & Security;28(3-4);130-7, (2009).
4. Qu J, Zenghua Zhao, Lianfang Zhang, Yantai Shu."Optimizing Aggregate Throughput in 802.11 Networks through Balancing Spatial Reuse and Transmission Rate", Global Telecommunications Conference 2009;1-5. (2009).
5. Leung A, Sheng Y and Cruickshank H "The security challenges for mobile ubiquitous services". Information Security Technical Report; 12 ( ); 162-171. .(2007).
6. N Garg & RP Mahaputra, "MANET Security Issues", International Journal of Computer Science and Network Security, Vol 9, No 8, August 2009.
7. Chi K, Jiang X, Horiguchi S., "Joint Design of Network Coding and Transmission Rate selection for Multihop Wireless Networks". IEEE Transaction On Vehicular Technology; 59(5); 2435-2444. (2010)
8. Corson S and Macker J. "Mobile and Ad hoc networking (MANET); Routing Protocol Performance Issues & Evaluation Considerations.RFC 2500." (1999)
9. Diaa Salama, Hatem Abdual Kader, and Mohiy Hadhoud, "Wireless Network Security still Has No Clothes.", 7th International Conferences Informatics and System, Cairo, 28 Mac – 30 Mac 2010, pp 1-8. (2010)
10. KB Chang, "Intelligent Control and Automation Lecture Notes in Control and Information Sciences", 2006, Volume 344/2006, 138-143, DOI: 10.1007/978-3-540-37256- 1_18.
11. Kitahara H, Okada H, Mase K., "Experimental Evaluation of a Novel Transmission Rate Assignment Scheme in Wireless Mesh Networks". 7th IEEE Consumer Communication and Networks Conference, 1-5.
12. Bruno P. S. Rocha, Daniel N. O. Costa, Rande A. Moreira, Cristiano G. Rezende, Antonio A. F. Loureiro, Azzedine Boukerche, "Adaptive security protocol selection for mobile computing". Journal of Network and Computer Applications, Volume (33), pp569-587. (2010)
13. *H Yang*. *H* Y. Luo. F Ye. S W. Lu. L Zhang. *H Yang*, "security in mobile ad hoc networks"; challenge and solutions, IEE Wireless Communications, February (2004).

5/15/2012