International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Key Agreement Protocol Based On EC-MQV Algorithm for Cooperative Wireless Communication

Anagha Dhargave[1], S. U. Nimbhorkar[2]

[1, 2] Department of Computer Science and Engineering, G. H. Raisoni College of Engineering, Nagpur, India

Abstract: ***In wireless communication user cooperation is important because in wireless communication number of nodes is available in the network. It is seen that in normal wireless communication the performance is not good as compare to the cooperative communication, where cooperation among multiple nodes presents in the network and hence it is the topic of interest for most of the researchers. Although some of the wireless communication system is not uses cooperative, nature of communication and may cause a performance reduction since the node not trusted or it may prone to some of the attacks. To solve these issues in the wireless communication where number of nodes presents in the network, a simulation model is proposed based on Elliptic Curve Manezes Qu Vanstone algorithm (EC-MQV). In the proposed work the comparison between simple wireless communication and cooperative wireless communication is presented. The work used EC-MQV algorithm further to support the security of existing key agreement protocol. It is found that used of Elliptic curve also helps to improve the efficiency of the network.***

Keywords: Cooperative communication, EC-MQV algorithm, Information security, low power network, Wireless communication.

1. Introduction

Cooperation is the processes where multiple nodes join the network and communicate together instead of working separately, such a concept have been adopted because when the system uses simple network it is seen that the performance of the network is degrade [6] [9]. This is because in wireless communication the number of nodes is presents and these nodes are mobile, and every time it needs to search the network hence the more energy is needed [9]. So by understanding such issue the idea of cooperation raised, and becoming the topic of research. This cooperative wireless network supports the user mobility and enhances the capacity of network as well as provides the better performance than simple wireless network. For security of the communication such as in wireless communication number of nodes is present within the range, and in that some of them are not trusted nodes [6]. So for this purpose key agreement protocols are designed. The proposed work is implemented on basis of Elliptic curve Manezes Qu Vanstone algorithm [10]. Key agreement [7] is categorized into two algorithm namely Diffie Hellman and Manezes Qu Vanstone algorithm. In the next section the comparison between the two known algorithms is provided.

In most of the cases the work focuses on the communication only, then at that time the issue of security is neglected, and hence the problem in security of information may occur. So for this purpose to secure the communication this idea of cooperation raised. There are different schemes for cooperation depends on the condition. They are amplify and forward, decode and forward, and compress and forward. These are techniques which are uses when the intermediate nodes are involved between source and destination communication. The scenario is shown in the figure below where the relay or intermediate node is present between source and destination node, also called as three node communication [4].

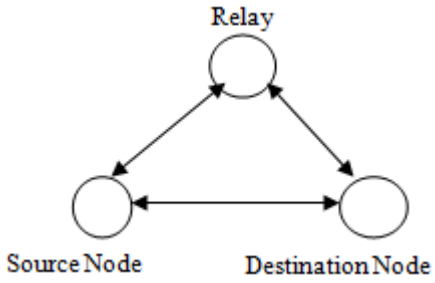

Figure 1: Three Node communication

In above scenario sometimes it may happen that eavesdropper can access the information by attacking on the relay node, and can involve in the further communication as a trusted node. So now a day cooperative communication is used by most of the system. Key agreement is basically used to provide the security to the communication where the trusted parties are agreed upon the session key and then established a communication. The study shows that to provide security to the communication Elliptic Curve Cryptographic (ECC) algorithm is powerful [3] [5]. This is like RSA algorithm that is public key cryptography but the results of ECC algorithm is better than RSA algorithm where in this smaller key size as compare to RSA algorithm is observed. In the Elliptic Curve both the algorithm that is Elliptic Curve Manezes Qu Vanstone algorithm and Elliptic curve Diffie Hellman algorithm are provide the better result.

The need to design the protocol is that when the wireless communication is occurred there may be chances of leak of information through the intermediate nodes, and hence to support the security of already implemented protocol the proposed word is designed. The work focused on the performance of the communication and more on the security of the transmitted designed the system where three nodes are

presents namely a source, a destination node and a relay or intermediate node. In this if the relay is not trusted or prone to various attacks then the communication is not secure.

2. Related Work

The proposed work is divided into three phase that is cooperative network, comparison between the cooperative network and simple network and lastly the implementation of the MQV algorithm. To design the work the study on different key agreement protocol in the wireless network had been done and work also analyzes the flaws of previous protocol as that the proposed work can produce better result and can support the existing work.

2.1 Cooperative Wireless Communication

The word cooperation means to share resource as well as support the communication so that performance of the overall system can be improved. This cooperative communication may lead most of system to enhance the performance and use less energy. Most of the researcher focuses on this because in wireless network the nodes are mobile in nature so the point of energy and bandwidth is raised. By using the concept of cooperation communication if in the network any of the node may experience such a problem then it can used the other node resources and hence communication cannot be stopped like other simple network. The cooperation can be carried out using the three strategies that is amplify and forward, decode and forward, and compress and forward. All the three techniques are depends on the condition of the source and destination node also on the intermediate node. Cooperative mesh network is also used by most of the system since the combination of the mesh network and cooperative network drawn the benefits for wireless communication.

2.2 Elliptic curve cryptography algorithm

The ECC is technique which was first designed by victor miller and Neil Koblitzs in 1985 for the public key cryptography offers application such as electronic mail, online security mechanism and many more [2] [7]. As there is fast development in the algorithms of public key cryptography use of it also increase. Day by day the changes in the algorithm motivate the scholar to use it for the better performance, this also offers higher security. For key agreement ECC offers the two known algorithm, namely ECMQV and ECDH [10].

Elliptic Curve Diffie Hellman algorithm (ECDH):
Traditionally used ECDG key agreement is based on elliptic curve in which no previous communication is made. Both that is sender and receiver generates public as well as private key then exchange public keys. After this the one of participant of communication combining its private key with other participant public key to performed secret communication. The figure below shows working of ECDH.

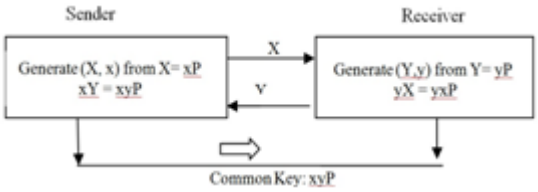

Figure 2: Working of DH key agreement algorithm

As shown in the figure sender and receiver agree to use Diffie Hellman to exchange secret information, here sender generate a session key (X,X) From random keys (x) and calculate X= xP where x is integer and X is elliptic curve point. Similarly receiver generates the session key as shown in figure. Sender sends X to receiver and receiver sends Y to sender and then both of them calculates xY=xyP and yX =yxP respectively. In this algorithm the problem is that there is not any proof that the information is reaching to the trusted receiver.

Elliptic Curve Manezes Qu Vanstone Algorithm (MQV): The MQV addresses issues in the Dh key agreement algorithm. In this algorithm communication is already established by exchanging trusted copies of data. After this both the participants of the communication exchange their dynamic public key and private keys. When the public key is received by both the party's they calculate some value using their own private key and other party's public key.

In this way the communication is established. In it if any disturbance occurs such as generated value from the public key and private key is not matched then the key agreement not takes place. This will help to improve the security of the elliptic curve algorithm. If anyone try to access the information then it will not possible because the secret key is not matched.

3. Implementation and Methodology

The proposed work is implemented key agreement based on elliptic curve MQV algorithm. To accomplished this the work is compromised in three different phases, in the first phase cooperative communication is shown where number of nodes are present and the information is transmitted using the nature of cooperative communication that is multiple node are used to transfer the data. In the next phase for practical purpose the comparison between cooperative and simple network is done and in the last phase the working of key agreement is shown. For the implementation of proposed work the simulation tool that is NS 2 is used. Network simulator is build on the basis of languages such as C++ and Otcl. Both the languages use for object orientation and for executing interpreter scripts [11]. To install the NS2, Linux or latest version of it that is ubuntu is need to install first. The following commands are needed to run on the ubuntu platform.
sudo apt-get install ns2
sudo apt-get install nam
sudo apt-get install xgraph

The proposed work used low power network such as adhoc wireless network [1] where all the nodes are formed

temporary network and there is no central administration [9]. In wireless network nodes are mobile so they act as routers for the other nodes to find path and also for access purposes. This network is useful when there is need of emergency communication or to share any data. The adhoc network is divided into two protocols they are table driven routing and on demand routing. The proposed work utilized adhoc on demand distance vector routing to find the path.

4. EC-MQV Algorithm

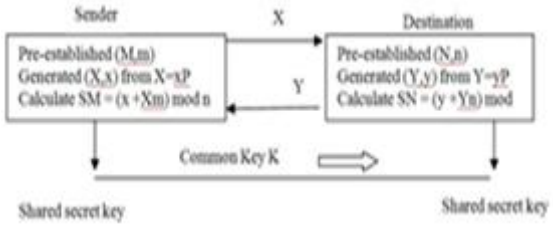

Figure 3: Working of MQV key agreement algorithm

In the MQV algorithm [8][10] as shown in the above figure 3 sender uses SM that is implicit value calculated as shown in the figure where n is the order of point (P) generation. The destination uses SN. Both sender and receiver shared secret key K. This can be calculated as follows,

$K = hSM (Y + yN) = hSN(X + xM)$

Where h is cofactor,

x and y denotes the first L bits of the first component X or Y respectively,

(M,m) – Public key and private key of sender

(N,n) – Public key and private key of receiver

(X,x) – Sessional key pair of sender

(Y,y) – Sessional key pair of receiver

Sender and receiver both send each other X and Y respectively, because the information is already exchange. In it the communication can guarantee that the information is received by intended receiver and provide the better security mechanism as well.

5. Results

The work is divided into three phases, in the first phase the cooperative network is formed where multiple nodes are present in the network and the node which are between the respective sender and destination are involved in the communication. This can help in the situation where one of the intermediate nodes is inactive so in that case other node involved in the communication can proceed the information further. The second phase presents the comparison between two networks. In the below figure it is shown that from the available nodes those who present in the communication range of source and destination are involved in the wireless communication, the formation of cluster is based on geographical position of the available nodes. For the comparison purpose the proposed work used the parameters such as packet delivery ratio (PDR), delay, time and throughput.

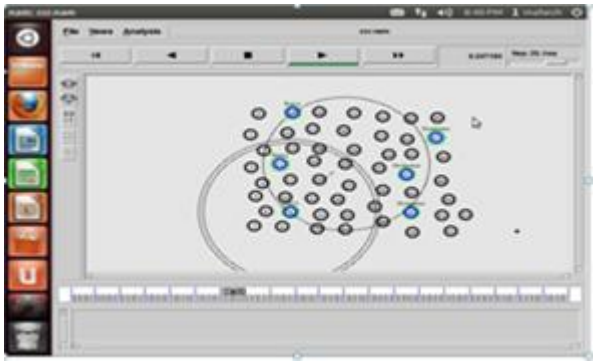

Figure 4: Communication of nodes

The above figure involves multiple source and destination for communication, where the communication between multiple nodes using the cooperative network is carried out. In the simple network it is seen that when the multiple nodes are involved in the wireless communication then if one of the node is inactive the information cannot process further and hence the delay is more as compare to cooperative network. As shown in the below figure where the network simulation compares the two networks and show that the performance of cooperative network is better than simple network.

The graph is used to compare the two networks, where the parameters such as delay and packet delivery ratio are calculated. PDR uses the formula in which the respective ratio between total packets transmitted from source to total receive packet at the destination side is find out. In this it is found that the PDR ratio is more in the proposed work as compare to simple network. The figure 6a and 6b show the parameter comparison of the two networks.

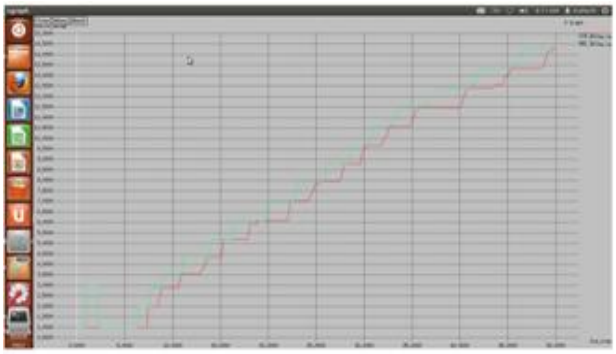

Figure 5: Comparison of End to End Delay

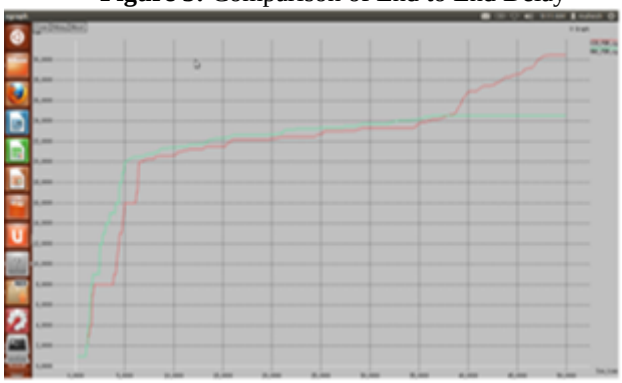

Figure 6: Comparison of packet delivery ratio

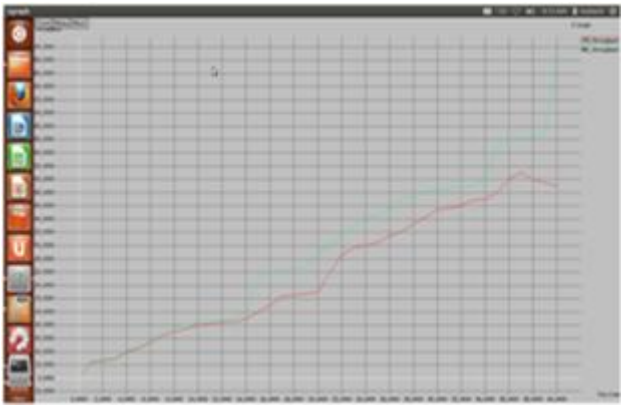

Figure 7: Comparison of throughput

The throughput can be calculated as per the requirement of the work. In the proposed work it is used to compare the two networks, based on the packets information from source as well as destination side. In the last phase dynamic scenario is shown where the selection of source and destination is depends on the user value. The work focused on the security as well as performance of the key agreement protocol.

6. Conclusion

The proposed work is based on ECMQV algorithm to implement the key agreement protocol for cooperative wireless communication; most of the key agreement protocol is based on the Diffie Hellman and other algorithm where there is no surety of information security. The proposed work make a use of cooperative communication for the better performance as discussed in the literature and in the results. From the study of the various algorithms for key agreement it can be conclude that ECMQV algorithm presents more secure communication. To compare the network designed work also used various factors and it is seen that the cooperative key agreement protocol for wireless network gives better performance using ECMQV algorithm and helps to enhance the efficiency of the system.

References

[1] Thomas R. Halford, Thomas A. Courtade, Keith M. Chugg "Energy- Efficient, Secure Group Key Agreement for Ad Hoc Networks" 2013 IEEE Conference on Communications and Network Security (CNS)
[2] Shaohui Zhu, Fan Yang, Liping Zhang, Shanyu Tang*, J Li "ECC-based Authenticated Key Agreement Protocol with Privacy Protection for VoIP Communications" 2013 ieee international conference on green computing and communications and ieee internet of things and ieee cyber, physical and social computing
[3] Jiyun Yang, Rui Zhang, Di Xiao" Analysis and Improvement of an Efficient and Secure Key Agreement Protocol" 2013 Ninth International Conference on Computational Intelligence and Security
[4] Ning Wang, Ning Zhang, T. Aaron Gulliver "Cooperative Key Agreement for Wireless Networking: Key Rates and Practical Protocol Design" ieee transactions on information forensics and security, vol. 9, no. 2, February 2014.
[5] Salama S. Ikki, P.Ubaidulla, Sonia Aıssa "Performance Study and Optimization of Cooperative Diversity Networks with Co-Channel Interference" IEEE transactions on wireless communications, vol. 13, no. 1, January 2014
[6] K Wang, M Wu "Cooperative communication based on trust model for mobile adhoc networks" published in IET information security, 2009.
[7] A Chandrashekhar, V Rajasekar, V Vasudevan "Improved authentication and key agreement protocol using ECC" international journal of computer science and security vol. 3
[8] Li Chin Hwang, Min-Shiang Hwang " An efficient MQV key agreement scheme" international journal of network security, Vol. 16, no. 2, Mar 2014.
[9] A. F. M. Shah, Md. Shariful Islam "A survey on cooperative communication in wireless network" international journal of intelligent system and application, June 2014
[10] "ECC challenges" certicom research, November 10 2009.
[11] "NS simulator for beginners" lecture notes, December 4, 2003-2004, France

Author Profile

Anagha S Dhargave is pursuing Master of Engineering (M.E.) in Wireless Communication and Computing (WCC) department of Computer Science and Engineering (CSE) from G.H. Raisoni College of Engineering, Nagpur, MS, India. She received Bachelor of Engineering (B.E.) degree in 2013 from RTMNU, Nagpur, MS, India. Her research interest areas are wireless communication, network security.

Sonali U Nimbhorkar received Post Graduate degree in computer science from RTMNU, Nagpur. She has published more than 30 papers in various international journals and international conferences as an main author and co-author in the field of issues related wireless network, wireless mesh network, network security and cryptography. At present she is assistant Professor in Computer Science & engineering. Department in G. H. Raisoni College of Engineering Nagpur, India.