International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 23 (2017) pp. 13933-13943
© Research India Publications. http://www.ripublication.com

Efficient routing and High security transmission using AODV and Distributed protocol key generation with Dual RSA

Rajaram Jatothu
Research Scholar, Department of Computer Science and Engineering,
Sri Satya Sai University of Technology and Medical Science, Sehore, Bhopal, Madhya Pradesh, India.
Orcid: 0000-0002-9245-6739

Dr. RP Singh
Professor, Department of Computer Science and Engineering,
Sri Satya Sai University of Technology and Medical Science, Sehore, Bhopal, Madhya Pradesh, India.

Abstract

Security is a major issue in mobile nodes communication, because of the various attacks like active attack, passive attack, internal attack, external attack, Blackhole (BH) attack, wormhole attack, Byzantine attack, eavesdropper and flooding attacks. This attack causes the various effects like data loss and packet loss. To overcome these problems and to provide higher security in Mobile Ad-Hoc Networks (MANET), Ad hoc On-Demand Distance Vector-Dual RSA-Quantum Cryptography (AODV-DRSA-QC) technique is introduced. In this AODV-DRSA-QC method, Cryptography method is employed for security purpose in between the source (Alice) and destination (Bob) with the help of Key values. In our AODV-DRSA-QC system, QC method is used for same encryption purpose and the cryptographic key is additionally encrypted through the dual RSA method as well as Advanced Encryption Standard (AES) is employed to encrypt and decrypt the message based on the Dual RSA key. AODV algorithm is employed for Routing purpose. The AODV-DRSA-QC method gives better results in terms of throughput, number of alive nodes, number of dead nodes, and energy compared to the existing systems.

Keyword: Security, Environmental attacks, Mobile Ad-Hoc Networks (MANET), Ad hoc On-Demand Distance Vector-Dual RSA-Quantum Cryptography (AODV-DRSA-QC), Advanced Encryption Standard (AES), Throughput, Number of alive nodes, Number of dead nodes and energy consumption.

INTRODUCTION

MANETs is one kind of self-configuring and dynamic wirelesses network that has numerous transferable consumer equipment. Mobile nodes are communicated with each other without any fixed central base station to monitor the nodes and to transfer data between the nodes [1, 2]. MANET is widely used for military purpose, personal area network, in a disaster area and so on [3]. However, MANET has many issues such as finite transmission bandwidth, broadcasting messages, reliable data delivery, these tablishment of the dynamic link and restrained hardware triggered processing abilities. In that, the security is the major problem because of the various attacks like active attack, passive attack, internal attack, external attack, BH attack, wormhole attack, Byzantine attack, eavesdropper and flooding attacks [4]. Many researchers have taken place to overcome the security problem in MANETs. The main issue present in MANET is the detection of the Malicious Node (MN) which minimizes the duplication of route requests in MANET by usingPolynomial-Reduction Technique [5].

MANET is vulnerable to malicious attacks. The sole reliance on wireless links, communicate nature of wireless transmission, dynamic topology, nonappearance of infrastructure, and multi hop routing has been recognized as the essential highlights that make MANETs vulnerable to malicious attacks. Security techniques for infrastructure-based networks are often not applicable to MANETs. For example, the use of a unique Certification Authority (CA) is beside the fundamental idea of infrastructure-less networks [6].Privacy denotes for security against unauthorized disclosure of information. Cryptography provides security for digital contents. Videos' streaming in real-time is sensitive to delay, involves encoding and decoding and has the smallest bandwidth and other Quality of Service (QoS) requirements [7]. Bullet Proof verification (BPV) method is one, which pins down the BH node by considering the two steps of the BH detection with the cryptographic mechanism. It does not use flooding to identify the BH node but it will not isolate the BH node from the network [8]. Secure Routing Protocol (SRP) that relies on DSR, is employed to certify the reliability of the identified route [9].

Authenticated Routing for Ad hoc Networks (ARAN) protocol employs public key cryptography to obtain the same result as SRP [10]. Security-Aware Ad-hoc Routing is a comprehensive protocol to identify the routes that encounter a certain safety criterion. The security criteria are met when the common Secret Key (SK) is shared to all nodes [11]. A certain security level is met when the SAR finds the path.

After the identification of the path, the ARAN and SRP are established. In all of these protocols, communicating nodes are easily discovered by the control messages and these control messages are handled by the intermediate nodes. Protecting the Anonymity of the communicating nodes is a challenge that needs to be addressed. The Onion Routing protocol addresses the issues of providing anonymous and secure communication [12]. An indirect communication method is provided among the applications by networked Computing nodes, these nodes are called as onion routers.There are some constraints present in the existing methods such as routing overhead, throughput, energy and security issues. To solve these issues, this paper has introduced AODV-DRSA-QC method. This AODV-DRSA-QC provides a higher secured method in MANET communication. In the normal security methods, Cryptography method is employed for security purpose in between the source (Alice) and destination (Bob) by way of Key values. In our AODV-DRSA-QC system, QC method is used for same encryption purpose and the cryptographic key is additionally encrypted by the way of dual RSA method. AES is also used for security purpose of MANET and the encrypted form of a message (Cipher text) is transmitted by using the AODV Routing. After reaching the destination, the message (Cipher text) is converted into plain text. The AODV-DRSA-QC method gives better results in terms of throughput, number of alive nodes, number of dead nodes, and energy compared to the AODV-QC method.

RELATED WORK

V. Manjusha and N. Radhika [13] introduced three various methods of BH detection and analyzed all the three detection methods in terms of throughput, energy consumption, and end-to-end delay. It gives the best results in terms of throughput as well as energy consumption but here it has a limitation in delay and overhead.

D. Hurley-Smith *et al.* [14] introduced the novel security protocol, Security Using Pre-Existing Routing for Mobile Ad hoc Networks (SUPERMAN). SUPERMAN protocol is implemented to network access control, address node authentication and secure communication for MANETs using existing routing protocols. SUPERMAN combines routing and communication security at the network layer. But the drawbacks are reduced average in end-to-end delay, packet drop, and average jitter.

D. Nguyen *et al.* [15] presented a mathematical model that allows foranalyzing the delay of epidemic broadcast in a MANET where packets have different levels of security requirement. The nodes performed a security association such as re-authentication, packet's requirement,network, mobility and trust models gives quite generic simulation results and also agree with the analytical results at different networking and mobility parameters such as density and node's velocity. Butthe security criterion is not discussed.

Y. Wang *et al.* [16] have given the huge amount of authorized MANET nodes and the interactions among the MN is modeled by introducing a mean field game theoretic approach for security in MANETs. Energy consumption and loss of security value are minimized by simulating the results with the authorized nodes which elect the distributed actions intelligently with optimal strategy. This method couldn't be applicable tomultiple attackers.

J.M. Chang *et al.*[17] has identified malicious nodes in MANETs by Cooperative Bait detection scheme (CBDS), under gray/collaborative BH attacks. The RREP reply message is delivered from the address of bait destination such as the address of an adjacent node to bait malicious nodes.The reverse tracing technique is used for detecting the MN. The nodes which have the BH attack does not exist while performing the routing process. If the route has BH attack, that route is terminated and the communication is stopped amid the network. The majorissuein the MANET iswhen the node's speed increases at the time throughput decrease.

AODV-DRSA-QC METHODOLOGY

The security is the major issue in any kind of wireless networks. In this paper, the AODV-DRSA-QC methodology is presented that provides the higher secured communication in MANETS. Also, the AODV-DRSA-QC system finds the BH attacks. The AODV-DRSA-QC system consists of ten major steps: 1) Mobile node development, 2) Transmission of data pocket, 3) Quantum Cryptography (QC), 4) Quantum Key (QK) encryption by using Dual RSA algorithm, 5) AES Encryption, 6) AODV Routing, 7) Detection of BH attack in Network, 8) Announcement of attack, 9) Successfully receiving the data to the destination,10) AES Decryption process. In the fig.1. Shows that the basic building block of AODV-DRSA-QC system.

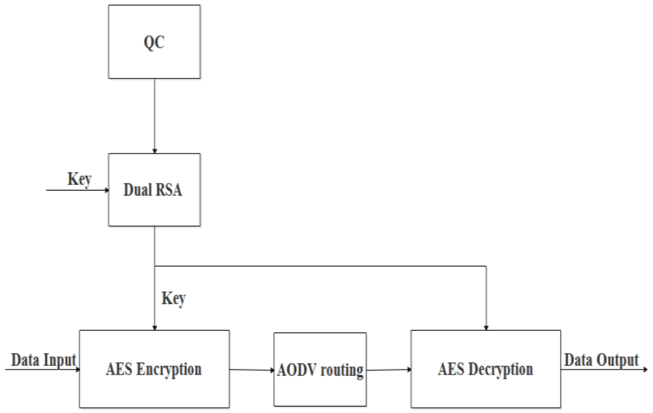


Figure 1: AODV-DRSA-QC methodology

The input data performs the quantum encryption more efficiently. After performing the encryption, the key will be generated. In this work, more security is introduced to perform cryptography. The generated key again encrypted with DRSA method. This DRSA encryption generates another key. That key is much essential to retrieve the original data in Quantum decryption block. The flow chart of the AODV-DRSA-QC system is shown in the below Fig. 2.

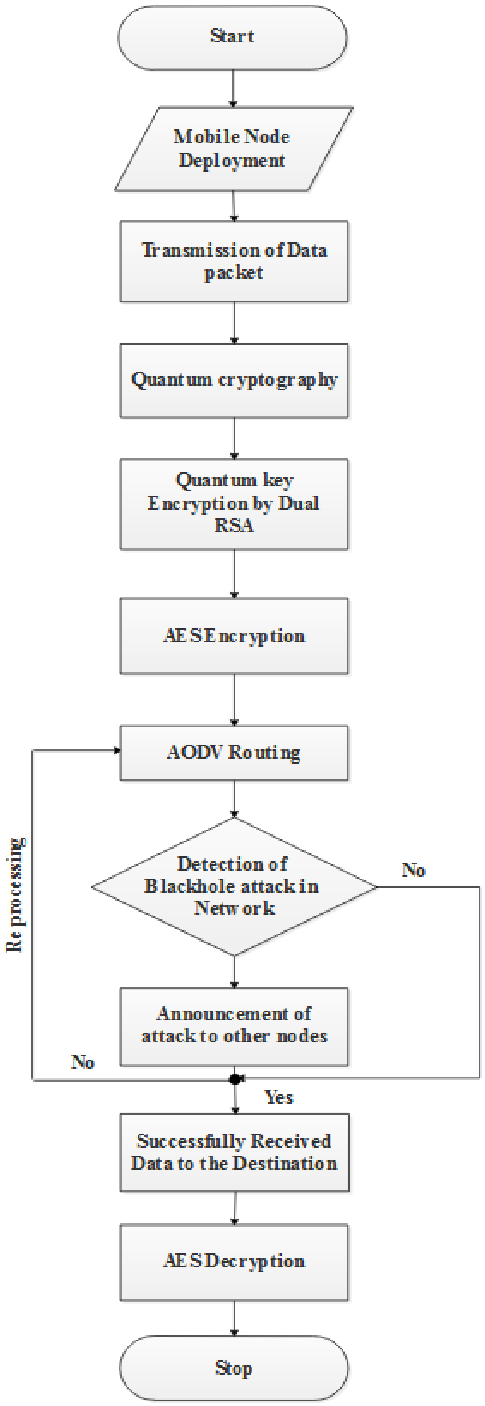

Start
Mobile Node Deployment
Transmission of Data packet
Quantum cryptography
Quantum key Encryption by Dual RSA
AES Encryption
AODV Routing
Detection of Blackhole attack in Network
No
Reprocessing
Announcement of attack to other nodes
No
Yes
Successfully Received Data to the Destination
AES Decryption
Stop

Figure 2: The flow chart of the AODV-DRSA-QC system

Mobile node development and Transmission of data pocket.

Initially, mobile nodes are positioned randomly in the interested area to establish the communication between the Source Node (SN) and the Destination Node (DN). From the SNs, the data packets are generated. The generated data packets are given to the cryptography section.

Quantum Cryptography

The data is transmitted confidentially among two parties such as Alice and Bob by the use of QC.Based on the quantum physics the key is introduced among Alice and to the Bob for making the highly confidential communications, it also relies on the classical information theory. The key that is produced in the QC, called as the Distributed Key (DK), this DK is common for both Alice and Bob and it becomes secret. By fusing the original data with the DK, the encryption process happens and the observer does not know the key. The decryption process is done by the copy of the key that is produced in the QC.

The quantum-DK and the encryption algorithm provide the security during the data transmission. If anyone of the link becomes broken, that link will regenerate with the help of QC. The confidential key is introduced based on the quantum mechanics laws; it has strange properties. Properties of quantum mechanics depend on the eavesdropping detectable. The eavesdropping is also called as an Eve that used to determine the key. The authorized parties are removed, when there is no information is delivered along the path. The DK confidentiality is ensured when there is no tapping is discovered. The second link of the chain has strange properties like the first link. The encryption key usedonly for transmitting the desired messages, it is not used for delivering the subsequent messages. Because the Quantum Key distribution (QKD) is used for distributing the long keys as often as needed by Alice and Bob.

QC based transmission in MANET

QC technique uses quantum mechanics for improving the confidentiality of the data communication in MANET. It uses a randomkey toencrypting and decrypting the information between the SN and DN. The major objective QKD is to detect the intrusion node and improves the secured data packet transmission Fig.3. Show the Block diagram of Quantum communication systems with shared SK for efficient data packet transmission from SN to DN.

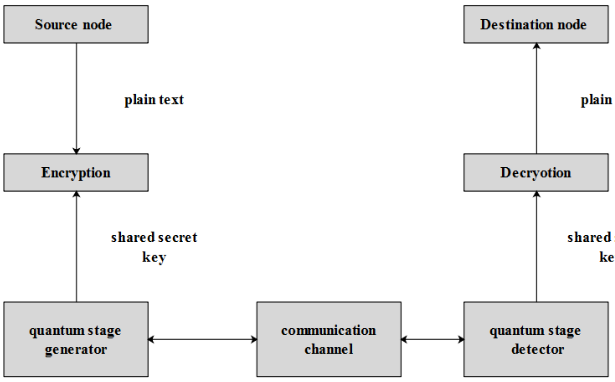


Figure 3: Block diagram of the quantum communication system with shared key

The QKD enables SN and DN to create a shared SK although there is a potential presence of an intrusion in MANET. In order to ensure the security, the QKD utilizes the accurate property of the quantum states. Quantum based key distribution is used for detecting the intrusion without disturbing the data packet transmission in MANET. A Quantum state generator creates the shared SK and then it distributes to source for encryption. Also, it distributes the same key to the quantum state detector at the destination side for decryption. Both the SN and DN keep the SKin contact to achieve the perfect SK for transmission in a significant manner The Quantum communication involves the encryption process in quantum states or qubits.

The SN and DN are connected by a quantum communication channel which permits the quantum states to be transmitted. Generally, four possible states are available such as (|0> + |1>), (|0> - |1>), |0>, |1>. During the transmission, the input bits of the data packets are transmitted. After that, randomly selected bases (rectilinear or diagonal) are used to convert the binary bits into qubits. The quantum approach uses two polarization states namely, the rectilinear basis or the diagonal basis.

SN generates an input bit either 0 or 1 and then chooses any one of the bases (rectilinear or diagonal) to transmit the information. Then the connectionbetween the qubit and binary bits are expressed as follows,

Basis	Bits	
	0	1
Rectilinear basis (+)	⇧	⇨
Diagonal basis (x)	⬀	⬂

Table 1: Relationship between the qubit and binary bits

Source node random bit	0	1	1	0
Phase shift	0°	180°	180°	0°
Designation node measurement based	0	0	1	1
Shared secret key	0	-	1	-

From the table 1, the two polarization states are explained with qubit and a binary bit. The node has the capacity for discovering the third party (i.e. intrusion) which trying to obtain the knowledge of the key and utilization of the QC. The SN key is encrypted with the above said nonorthogonal states of the information and it sends to the DN which results in increasing the secured data packet transmission at the DN end.

The information is phase shifted by 0° and 180° with separated time and the difference in their time is Δt .The information of encryption is transmitted to the quantum state detector through the communication channel. After that, the encrypted information is decrypted by the way of shared SK (i.e.0 or 1). The different possibilities of phase shifting are measured by sender and DN with two measurement bases such as rectilinear basis and diagonal basis. The two non-orthogonal bases consist of four possibilities is clearly described as follows.SN encrypts the information bit 0 in the quantum state by using a Phase shift (PS) of 0° and DN measurement basis is also with a PS of 0°.Then it concludes that the information is encrypted in 0 is the one-time unit.

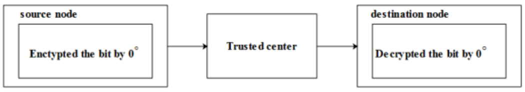


Figure 4: PS by SN is 0° and PSby designation node 0°

Fig.4. illustrated the similar PS is obtained among the SN and DN. Therefore, the information bit is transmitted in a secured manner. The next possibilities are that the source encrypts the bit 0 in the state by using a PS of 0° with the time unit. Then the DN provides the incorrect measurement due to a PS of 180°. This indicates that the measurement basis was wrong due to which the information is lost and it does not conclude whether the transmitted information was 0 or 1. From the result, the key is not matched between the SN and DN. Therefore, the intrusion node is identified and packet dropping is reduced in MANET. The above process is described in fig.5.The third case is that source encrypts the bit 1 in a quantum state with the PS of 180°. Similarly, the DN decrypt the bit with the measurement basis is correct, i.e., a PS of 180°. The schematic diagram of the Quantum PS (QPS) approach is shown in Fig.6.

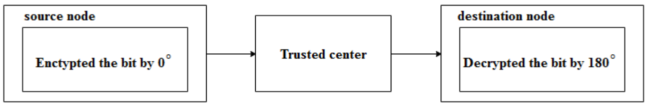


Figure 5: PS by SN de is 0° and PS by designation node 180°

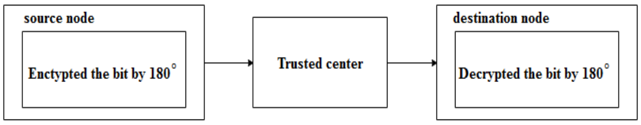


Figure 6: PS by SN is 180° and PS by designation node 180°

From the fig.6. QPS is obtained between the SN and DN with the similar secret key. The figure shows that the information is encrypted and the phase shifted by 180° and hence correct information is observed at the DN. The DN measures the phase of the information and it concludes that the encrypted data as 1. The final case is that source encrypts the information bit 1 in a quantum state with 180° phase shift. However, the DN measurement basis is incorrect, i.e., a PS of 0°. Fig.7. shows the QPS measurement.

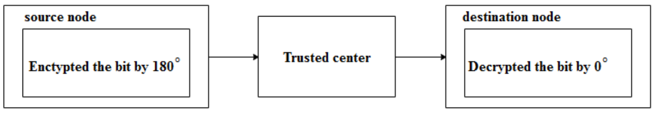


Figure 7: PS by SN is 180° and PS by designation node 0°

Fig.6 clearly illustrates the PS is obtained among the SN and DN. The information occurring at the destination side is wrong due to which the bit is lost and the system cannot state whether that information is 0 or 1.Therefore, the DN informs the source of the instances where it got accurate results. As a result, the source and DN keep these bits as their key bits and remove all the other bits. Table2 shows the generation of SK transmitted by the source and the measurement basis used by DN.

Table 2: Secret key for source and designation

Key Generation	
Select p, q	p, q
	both are prime $p \neq q$
	Calculate n = p*q
	Calculate $\emptyset(n) = (p-1)x(q-1)$
Select integer e	$gcd(\emptyset(n), e) = 1; 1 < e < \emptyset(n)$
	Calculate d
Public key	KU ={e, n}
Private key	KR={d, n}

Encryption	Decryption
Plain text M< n Ciphertext$C = M^e(mod\ n)$	Ciphertext C Plain text $M = C^d(mod\ n)$

Input: Source (S), Designation (R), Quantum key value 'QK_i = QK_1, QK_2, QK_3…QK_n', Data packets 'DP_i = DP_1, DP_2, DP_3…DP_n'. Input bits 0 and 1

Output: Improved secured data transmission

```
Begin
    If (S Encryption bit '0' and R measurement basis is 0)
        Resultant bit is '0'
    End if
    If(S encrypts the bit '0' and R measurement basis is 1)
        Resultant bit is cannot state '0' or '1'.
    End if
    If(S encrypts the bit '1' and R measurement basis is 0)
        Resultant bit is cannot state '0' or '1'.
    End if
    If(S encrypts the bit '1' and R measurement basis is 1)
        Resultant bit is '1'.
    End if
  Obtain the SK at the quantum stage detector
      If (the shared SK is matched at the DN)
            Secured transmission is obtained
      Else
            Transmission is declined
      End if`
End
```

The above algorithmic description is clearly described the secured data transmission from SN to DN in MANET. After the QC process, the key value is again encrypted and decrypted by using Dual RSA algorithm.

Quantum Key encryption by using Dual RSA algorithm.

For higher security communication, in this section Quantum key is encrypted by using Dual RSA algorithm. For making the encryption and decryption, the RSA algorithm is employed in modern computers. It is an asymmetric cryptographic algorithm and it has two different keys. The

RSA has three algorithms: key generation, encryption, and decryption.

RSA Algorithm

RSA cryptography is the popular cryptography system. It is used for the security purpose in the wide range of networks. In the RSA, the boundary of security should be raised. The public and the private key-generation algorithm is the most difficult part of RSA cryptography. RSA cryptography is employed for generating the two large prime numbers p and q. A modulus n is calculated by multiplying p and q. The link among the users is established by the numbers that areemployed for both the public and private keys. The one user sends plain text to the encrypted public key.

Dual RSA

The Dual RSA is basically two distinct instances of RSA that shares the same public and private exponents. To obtain the one Dual RSA, combines the two instances of the RSA with thepublic key (e, N_1 ,N_2) and private key(d,p1,q1,p2,q2), where e and d satisfy $ed \equiv 1 \bmod (\phi(N_1))$ and $ed \equiv 1 \bmod (\phi(N_2))$. From these two relations, it obeys that there exists two positive integer k_1 and k_2 such that

$$ed \equiv 1 + k_1\phi(N_1)$$

$$ed \equiv 1 + k_2\phi(N_2) \qquad (1)$$

Where, equation (1) is called as the Dual RSA key equations. The major concept of key generation algorithms presents in dual RSA that comes from the equation $k_1\phi(N_1) = k_2\phi(N_2)$ .it directly follows from the key (5). The scheme is constructed by using three integers like k_1, k_2, and k_3. The formula for DRSA key generation is represented as, k_2k_3 =(p1-1)(q1-1) and k_1k_3=(p2-1)(q2-1), where p1,q1,p2, and q2 are all prime numbers.

ADVANCED ENCRYPTION STANDARD (AES)

AES has two processes: AES encryption and AES decryption. These processes are employed to change the original message (Plain text) into ciphertextand ciphertext message into plain text. This AES method has employed for secure transmission in MANET.

AES encryption

AES algorithm used for the security purpose as well as it improves the speed. This AES encryption transforms the information into unintelligible form named as ciphertext and also it has ten rounds of encryption. Each round has four processing steps such as sub bytes transformation, shift rows transformation, mix columns transformation and add round key transformation. The rounds from one to nine are alike to the tenth round, which eliminates the process of mix columns.

Sub bytes transformation

Sub bytes transformation is a non-linear byte of substitution and it is operating at each byte of the substitution box. This substitution box is named as S-box.

Shift rows transformation

In shift rows, each row of the state is rotated by an offset and the actual value of the offset is equal to the row index.

Mix columns transformation

Columns of the state are transformed by mix columns and those columns of the state are deliberated as polynomials over GF (28).

Add round key transformation

State array of the mix columns transformation is added with a round key in add round key process and it corresponds to an XOR-operation.

AES decryption

AES decryption extracts theplaintext (original form) from the ciphertext, which is generated by the AES encryption. This AES decryption is accomplished by reversing all steps of AES encryption with inversing functions like inverse shift rows, inverse substitute bytes, add round key, and inverse mix columns. Inverse substitute bytes have XOR output (add round key operation) of previous two steps with four words from the key schedule and the inverse mix columns do not commit with the decryption process.

AODV-ROUTING PROTOCOL

The routing protocol is intended for using mobile nodes in the ad-hoc network. The AODV is designed to decrease the dissemination of overhead and control traffic. The AODV routing protocol deals with two functions such as Route Maintenance and Route Discovery. The findingof the fresh route is decided by Route Discovery function and the discovery of link breaks and repair of an existing route is decided by Route Maintenance function. The reactive protocol does not maintain permanent route table. AODV is quickly able to analyze the changes in network topology. The data transfer process of AODV routing protocol is shown in Fig.8.

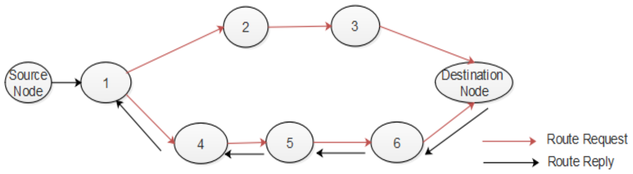
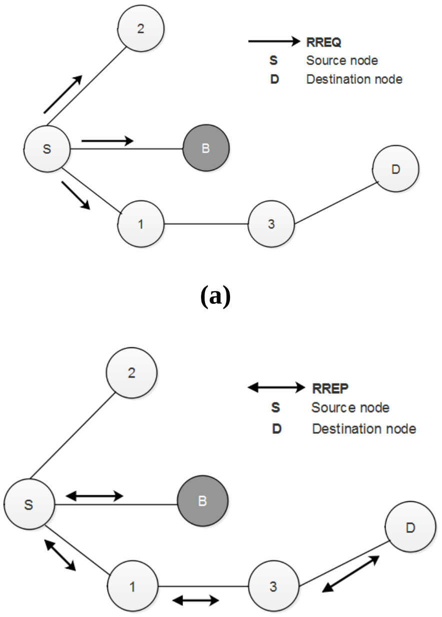


Figure 8: AODV Routing Protocols-Data Transfer

Detection of BH attack in Network.

The black-hole node responds blindly to every Routing Request (RREQ) with the huge sequence number and least hop count values to convince the SN that has a new route to the DN. In this AODV-DRSA-QC method, the AODV routing is used for discovering transmission path between the source to the destination without any BH attack present in the path. BH attack means, the path with heavy packet losses in a transmission. If any path has BH attack means that has to be discarded and the new route is to be formed based on the AODV consideration. BH attack is discovered based on the energy present in each node of MANET. At first, the SN delivers the request to the neighbor's node based on the threshold range that is fixed in the network. If the node has adequate energy for transmitting the data, that node has taken for creating the transmission path or else this node has to be discarded from the transmission. By avoiding the node with less amount of energy, the BHis reduced and the amount of information transmitted in the MANET is increased.



(a)

(b)

Figure 9: (a) Route request and (b) Route reply in the presence of BH node B

Fig.9. shows the route request and route reply process of AODV routing protocol. The final process of our AODV-DRSA-QC system is Announcement of attack and successfully receiving the data and decryption process.

ALGORITHM

In our contribution, the quantum cryptography method such as QKD generates two types of keys such as Alice and Bob keys. These keys are taken as the input for Dual RSA encryption and decryption process. Public and private keys are generated by the Dual RSA method. Advanced Encryption Standard (AES) is employed for encrypting and decrypting the messages and it takes two types of inputs such as the output of the Dual RSA algorithm and the message that want to encrypt and decrypt. AODV routing is used to transmit the message along the MANET.

Quantum cryptography

QKD is the best method in the quantum cryptography. BB84 protocol is used for generating the Alice (Sender) and Bob (Receiver) keys. These keys are used with Dual RSA algorithm to encrypt and decrypt the messages.

BB84 algorithm

1. Random bits are generated by the sender in the range of$(4+\beta)m$.
2. Random$(4+\beta)m$- bit string c is elected by sender. For each bit, the sender generates the state in the range of $|0\rangle, |1\rangle$ at $c = 0$or $|+\rangle, |-\rangle$at $c = 1$.
3. The sender transmits the resulting qubits to the receiver.
4. The $(4+\beta)m$ qubits are collected by the receiver, computing each in$|0\rangle, |1\rangle$ or$|+\rangle, |-\rangle$ based on random.
5. c announced by sender.
6. If sender delivers on the different basis the receiver discards value. In high probability, there are at least $2m$ bits are left. In this protocol, sender chooses randomly on a group of $2m$ bits and elects at random m of these to b check bits.
7. Check bit values are declared by the sender and receiver. It aborts the protocol when few of these values agree.
8. Sender declares $p+q$, where p is a random code word in D_1 and q is the string consisting of the remaining non-check bits.
9. Receiver subtracts the $p+q$ from its code qubits,$q+\in$, and corrects the result, $p+\in$, to a code word in D_1.
10. Sender and receiver employs the coset of $p+D_2$ as the key.

Dual-RSA algorithm

$k1$ and $k2$ are the two positive integers existed in this algorithm.

$ed = 1 + k1\,\Phi(n1)$ and $ed = 1 + k2\,\Phi(n2)$

1. $p1, q1$ and $p2, q2$ are the elected four distinct prime members.
2. Calculate $n1 = p1 * q1$ and $n2 = p2 * q2$
3. $\Phi\,(n1) = (p1 - 1) * (q1 - 1)$ and $\Phi\,(n2) = (p2 - 1) * (q2 - 1)$ are computed.
4. An integer $'e'$ is elected between $\Phi\,(n1) < e < \Phi\,(n2)$ and the $GCD\,(e, \Phi\,(n1), \Phi\,(n2)) = 1$ are relatively prime. Public key exponent is released in the form of "$e, n1, n2$".
5. Compute $d1$ and $d2$. Where, $ed1 \equiv 1(mod\,\Phi\,(n1))$ as well as$ed2 \equiv 1(mod\,\Phi\,(n2))$. Here $d1$ and $d2$ lies in $0 < d1 < n1$ and $0 < d2 < n2$ respectively. Private Key exponents in the form of"$d1, d2, p1, q1, p2, q2$".

AES algorithm

AES has two processes such as AES encryption and AES decryption for converting the plain text to Cipher text and Cipher text to plain text respectively.

AES encryption algorithm

1. Group of add round keys from the cipher key.
2. The state array is initialized and the initial round key is added at the beginning state array.
3. After performing the round from 1 to 9, the usual round such as a) Sub bytes, b) Shift rows, c)Mix columns and d) Add round key, using K (round) is executed.
4. The final round is executed such as a) Sub bytes, b) Shift rows and c) Add round key, using K (10).
5. At final round step, the corresponding ciphertext is extracted.

AES decryption algorithm

Inverse the round transformations of AES encryption process such as a) Inverse shift rows, a) Inverse sub bytes, c) Add round key and d) Inverse mix columns is performed to change the original form of the input message (Plain text).

The third step contains the XOR-ing output of the previous two steps with four words forms the key schedule. Inverse mix columns don't perform at the last round key.

AODV routing algorithm

The route is generated among the source to the destination based on the four types of control messages such as Routing Request Message (RREQ), Routing Reply Message (RREP), Route Error Message (RRER) and HELLO messages.

1. RREQ is a kind of request message and it is delivered by a node for knowing a route to another node.
2. RREP is replied message of RREQ and it is only in a unicast direction.
3. The nodes deliver the notification via RRER message when the nodes are lost their link amid the transmission.
4. Finding and monitoring the connections of the neighbors is carried out by the HELLO messages.
5. Finally, the route is created from the source to the destination.

RESULTS AND DISCUSSIONS

AODV-DRSA-QC system was implemented by using MATLAB 2017a software tool (for the simulation purpose) through the i5 desktop computing environment with 8 GB RAM memory capacity. In that AODV-DRSA-QC, the quantum cryptography and dual RSA used for security purpose and the routing areprovided by the AODV protocol. The following Table 3 shows the simulation parameters which is used in the AODV-DRSA-QC methodology. For knowing the better performance of this AODV-DRSA-QC method, it is compared with the AODV-QRC method.

Table 3: Simulation parameters

Parameter	**Value**
Area	250*250 m^2
Sensor nodes	200
Initial energy of sensor nodes	0.5 J
Number of simulation iterations	Length(message)
Communication rangefrom each node	50 nm
E_T	0.2 PJ/bit/ m^2
E_R	0.1 PJ/bit/ m^2
Packet size	4000 bits
Message size	200 bits

Alive nodes

The node which has an adequate amount of energy for transferring the information (Cipher text) is named as alive nodes. A number of alive nodes become high, for an effective data transmission in MANET.

Dead nodes

The nodes which don't have any energy for transmitting the information is called as dead nodes. It degrades the performance of the entire network, as well as the dead nodes, should be less for avoiding the packet loss.

Energy consumption

The totalquantity of energy required for each node to deliver the message (Cipher text) through the path is extracted in the AODV routing and the total energy consumption is given in equation (2),

$$E_c = E - (E_T - E_R) \quad (2)$$

Where energy consumption of the MANET is represented asE_c, E is defiend as the total amount of energy, the transmitting and receiving energy is represented asE_T and E_R respectively.

Throughput

Throughput is described as a number of successful messages delivered to the destination as well as this value should be high for an effective data transmission. The following equation (3) is given for measuring the throughput in a MANET.

$$T_H = N_T \times P_L \quad (3)$$

Where, $T_H$is denoted as throughput of the MANET, total number of rounds as denoted as N_T and the packet length is represented as P_L.

Table 4. Shows the comparison between the AODV-DRSA-QC and AODV-QC methodologies. It shows the comparison in terms of number of rounds vs the performance parameters such as number of alive nodes, number of dead nodes, energy consumption and throughput. From that table, conclude that the number of alive nodes of AODV-DRSA-QC is increased compared to the AODV-QC method. It improves the lifetime of the MANET. Dead nodes are decreased in that AODV-DRSA-QC method, it leads to decreasing the failure of transmission between the networks. These dead nodes are not taken while creating the transmission path in a network, because these nodes are caused the packet loss in the network. Load balancing among the source to the destination decides the energy consumption of an entire network. If the load balancing is high, it also increases the energy consumption of MANET. Compared to the AODV-QC, throughput of AODV-DRSA-QC method has greater performance .It shows the amount of packets delivered from source to the destination is high as well as the packet loss in a MANET is low.

Table 4: Performance measures of AODV-DRSA-QC and AODV-QC

Number of rounds	**Alive nodes**		**Dead nodes**		**Energy consumption (J)**		**Throughput**	
	AODV-QC	**AODV-DRSA-QC**	**AODV-QC**	**AODV-DRSA-QC**	**AODV-QC**	**AODV-DRSA-QC**	**AODV-QC**	**AODV-DRSA-QC**
20	102	108	96	92	8	18	2.4 e^3	3.5 e^3
40	85	99	115	100	-10	12	1.9 e^3	2.3 e^3
60	82	97	118	103	-28	4	1.5 e^3	2e^3
80	77	90	122	109	-46	-2	1.2 e^3	1.4 e^3
100	77	86	122	114	-64	-12	0.7 e^3	1.0 e^3
120	77	82	122	118	-80	-20	0.2 e^3	0.5 e^3

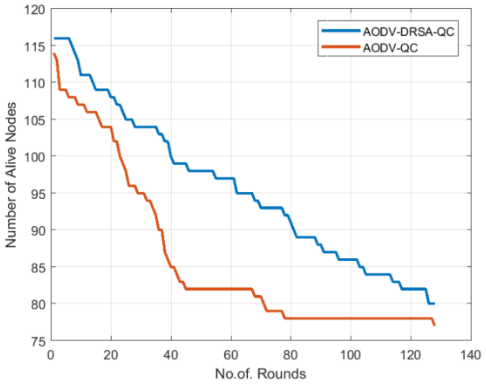


Figure 10: Comparison of alive nodes

Fig.10 shows the comparison of alive nodes in two methods such as i) AODV-DRSA-QC, ii) AODV-QC. From the graph, it is concluded that the AODV-DRSA-QC has a large number of alive nodes compare to the AODV-QC method. A huge number of alive nodes helps to transmit the information (Cipher text)for more time.

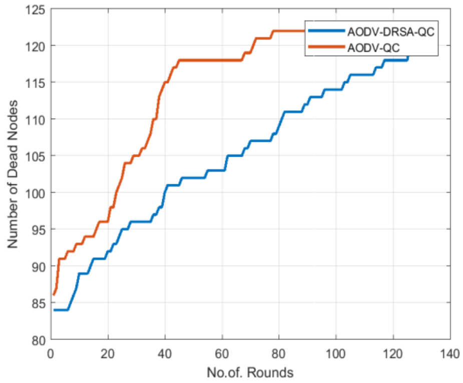


Figure 11: Comparison of dead nodes

Fig.11 shows the comparison between two methods AODV-DRSA-QC and AODV-QC in terms of dead nodes. The nodes become a deadnode when the nodes are fully drained their residual energy in a transmission. By comparing two methods, the number of dead nodes is minimized in the AODV-DRSA-QC method. Less number of dead nodes causes the packet loss should be low and also the BH attack is minimized.

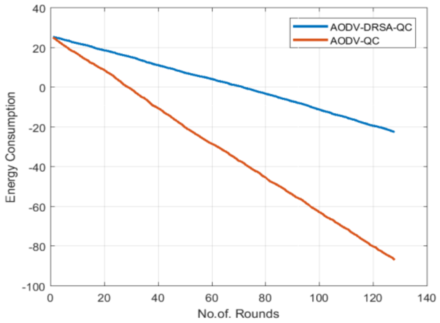


Figure 12: Comparison of energy consumption

Fig.12 shows the energy consumption of two methods AODV-DRSA-QC and AODV-QC. Energy consumption of the AODV-DRSA-QC is more compared to the AODV-QC method. Energy consumption is more when the load balancing amid the transmission path becomes high.

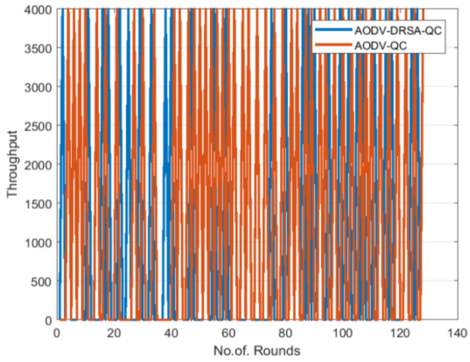


Figure 13: Comparison of throughput

Fig.13 shows the comparison of two methods AODV-DRSA-QC and AODV-QC in terms of throughput. From the analysis, it is concluded that the throughput of the AODV-DRSA-QC is increased. The throughput of the entire network is maximized by making the successful transmissions without any packet loss.

CONCLUSION

In this paper, an efficient Ad hoc On-Demand Distance Vector-Dual RSA-Quantum Cryptography (AODV-DRSA-QC) technique is introduced. In order to improve the secured data transmission, the QPS approach based data communication is designed for encoding the information input bit. The QKD utilized certain properties of quantum states and Dual RSA method has been introduced for improving the security and also detecting the BH attack without disturbing the data packet transmission in MANET. The Quantum based approach employs the phase shifting operation between the source and destination side through the SK distribution that helps to enhance the security of packet transmission with minimum overhead. The data is transferred by using AODV routing. The AODV-DRSA-QC technique has greater performance compared to the AODV-QC method as well as the performance is analyzedin terms of the number of alive nodes, number of dead nodes, energy consumption and throughput. In future, the AODV routing will be improved by the optimization technique for increasing the efficiency and the network life time of MANET.

REFERENCES

[1] Ranjan, Rakesh, Nirnemesh Kumar Singh, and Ajay Singh., “Security issues of black hole attacks in MANET”, IEEE, Computing, Communication &

Automation (ICCCA), International Conference on. 2015.

[2] Sardana, A., Bedwal, T., Saini, A., &Tayal, R., “Black hole attack's effect mobile ad-hoc networks (MANET)”, IEEE, In Computer Engineering and Applications (ICACEA), International Conference on Advances in, PP. 966-970, 2015.

[3] Burbank, J. L., Chimento, P. F., Haberman, B. K., & Kasch, W. T., “Key challenges of military tactical networking and the elusive promise of MANET technology”, IEEE Communications Magazine, VOl.44, Issue.11, 2006.

[4] Pooja Mishra and Ashutosh Rastogi “Security Issues and Attacks In Mobile Ad Hoc Networks”.

[5] Jayakumar, M., Newton, P.C. and DalvinVinothKumar, A., 2015, February. MIDURR: A technique to minimize the duplication of route requests in Mobile Ad-Hoc Networks. In Soft-Computing and Networks Security (ICSNS), 2015 International Conference on (pp. 1-4). IEEE.

[6] Djenouri, D., Khelladi, L. and Badache, N., 2005. A survey of security issues in mobile ad hoc networks. IEEE communications surveys, 7(4), pp.2-28.

[7] Perkins, D.D. and Hughes, H.D., 2002. A survey on quality- of- service support for mobile ad hoc networks. Wireless Communications and Mobile Computing, 2(5), pp.503-513.

[8] Ahmed, Firoz, Seokhoon Yoon, and Hoon Oh., “Bullet-proof verification (BPV) method to detect black hole attack in mobile ad hoc networks”, International Conference on Ubiquitous Intelligence and Computing., Springer Berlin Heidelberg, 2011.

[9] Papadimitratos, P. and Haas, Z.J., 2002. Secure routing for mobile ad hoc networks. In the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, January 27-31, 2002 (pp. 193-204).

[10] Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C. and Belding-Royer, E.M., 2002, November. A secure routing protocol for ad hoc networks. In Network Protocols, 2002. Proceedings. 10th IEEE International Conference on (pp. 78-87). IEEE.

[11] Yi, S., Naldurg, P. and Kravets, R., 2001, October. Security-aware ad-hoc routing for wireless networks. In Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing (pp. 299-302). ACM.

[12] Chaum, D.L., 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2), pp.84-90.

[13 Manjusha, V., and N. Radhika. "A Performance Analysis of Black Hole Detection Mechanisms in Ad Hoc Networks." Proceedings of the International Conference on Soft Computing Systems. Springer India, 2016.

[14] Hurley-Smith, D., Wetherall, J. and Adekunle, A., 2017. SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks. IEEE Transactions on Mobile Computing.

[15] Nguyen, D.Q., Toulgoat, M. and Lamont, L., 2016. Impact of trust-based security association and mobility on the delay metric in MANET. Journal of Communications and Networks, 18(1), pp.105-111.

[16] Wang, Y., Yu, F.R., Tang, H. and Huang, M., 2014. A mean field game theoretic approach for security enhancements in mobile ad hoc networks. IEEE Transactions on wireless communications, 13(3), pp.1616-1627.

[17] Chang, J.M., Tsou, P.C., Woungang, I., Chao, H.C. and Lai, C.F., 2015. Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. IEEE systems journal, 9(1), pp.65-75.