International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

QUANTUM BASED ADAPTIVE TOPOLOGY CONTROL FOR INTRUSION DETECTION AND ISOLATION IN MANET

E.Selvi[1], M.S. Shashidhara[2]

[1]Asst. Professor, Department of Computer Science, Asan Memorial College of Arts and Science, Chennai, India.
[2]Head of the Department, Department of MCA, The Oxford College of Engineering, Bangalore, India.

ABSTRACT:A mobile ad hoc network (MANET) is an infrastructure-less network where the number of mobile nodes is independently moved in a random direction within the transmission range of the network. Due to the movement of mobile nodes, the network topology is changed arbitrarily. Therefore, various intrusions are presented in MANET. For accurate and robust intrusion detection against several attack and deceiving actions, SIEVE technique was designed in MANET. However, node mobility of the ad hoc network restricts the BP algorithm efficiency and it's difficult to identify attack behavior. Therefore, security is a most important concern in decentralized structure of mobile network. In order to develop the intrusion detection and isolation in MANET, Quantum based Adaptive Topology Control (QATC) technique is developed. In QATC, an adaptive topology control is designed to adjust the transmission range of the mobile nodes to extend the lifetime of networks by retaining the network connectivity. This topology leaves maximum possible nodes connected in a cluster zone with minimum energy consumption and transmission interference. This helps to increase the packet delivery ratio. After this, the arriving and leaving nodes are monitored and the malicious node is identified from the network, through Quantum Mechanism. Quantum mechanism is typically used to detect the malicious node from the network using specific key distribution. Due to this, the malicious nodes are easily detected and isolated, aiming at improving the Malicious node detection rate with minimum time. A simulation result shows that the Quantum based Adaptive Topology Control (QATC) technique achieves higher packet delivery ratio, malicious node detection rate and reduces energy consumption, and time to identify the malicious node compared to state-of-the-works.

KEYWORDS: Mobile ad hoc network (MANET), malicious node, Adaptive Topological Control, Quantum Mechanism, intrusion detection, intrusion isolation

I.INTRODUCTION

A mobile ad hoc network is an infra-structure less network which can establish the route path through collection of intermediate mobile nodes. In MANET, the mobile nodes are randomly moved in any direction. Due to the mobility of node, the transmission range of the networks is varied accordingly. By varying the transmission range, several intrusions continuously attack the network's accessibility through common techniques such as flooding, black hole and denial of service (DoS). The mobile nodes perform packet transmission from one end to another end with the mobility of nodes and due to this wide range of intrusion occurs in MANET. Therefore, several review techniques are expensively developed.

MANET processed with two different types of modes such as single-hop and multi-hop. The nodes in MANETs assume that other nodes are always combined with each other to communicate data, which is exploited by malicious nodes and propagate intrusive attacks across the network. Intrusion detection system is developed for MANET to improve the security level and to detect the malicious attackers in the network.

To obtain accurate and robust intrusion detection against several attack and deceiving actions, SIEVE technique was designed in [1] to infer Identity of Polluters in MANET by exploiting Rate less Codes and Belief Propagation (BP). The BP algorithm evaluates the identity of malicious nodes residing upon the network with simple pollution detection mechanism. SIEVE technique ensures multi-party download or collaboration attack detection with minimal computational, memory and communication resources. However, node mobility of the ad hoc network restricts the BP algorithm efficiency, as it affects key Pre-distribution, identifying routing mechanisms and attack behavior.

To improve the routing performance in MANET, Energy-Aware Routing Algorithm was introduced in [2] along with RMECR and RMER. Reliable Minimum Energy Cost Routing (RMECR) addresses requirements of ad hoc

networks: energy-efficiency, reliability, and extending network lifetime. Reliable Minimum Energy Routing (RMER) is an energy-efficient routing algorithm which minimizes the route of total energy required for end-to-end packet traversal. However, the RMECR and RMER algorithm, for extending the network lifetime cannot be implemented for varying conditions.

The objective of the thesis is organized as follows. Quantum based Adaptive Topology Control (QATC) technique is introduced to develop the intrusion detection and effective isolation in MANET. Initially, an adaptive topology control technique is applied to adjust the transmission range of the mobile nodes to extend the lifetime of Adhoc networks by changing the network connectivity and improving the network lifetime. This topology also increases the packet delivery ratio and maximum possible nodes are connected in a cluster zone with minimum energy consumption and transmission interference. Then, the quantum mechanism is used to monitor and detect the malicious node from the network using key distribution followed by isolation of malicious nodes from the network for increasing the transmission.

The rest of the paper is organized as follows. In Section 2, a summary of different routing techniques to prevent intrusion in mobile ad-hoc network are explained. In Section 3, the proposed framework of Quantum based Adaptive Topology Control (QATC) technique with the help of diagram is described. In Section 4, simulation environment is provided with detailed analysis of results explained in Section 5. In Section 6, the concluding remarks are included.

II.RELATED WORK

Intrusion detection is a type of vulnerable attack in wireless mobile ad hoc networks that can occur during packet transmission between the mobile nodes. A new IDS scheme was introduced in [3] and selects novel cluster leader selection process and a hybrid IDS using Vickrey–Clarke–Groves which provides the intrusion detection service. However, it does not increase the intrusion detection rate. An approach based on a multivariate Hotelling's T2 statistical analysis technique was designed in [4] for intrusion detection in network environments. In [5], a lightweight system to discover the new characteristics of Sybil attackers with lack of centralized trusted third party. However, variable transmit powers and hidden attacks are the major issues in the network. A secure routing scheme was developed in [6] ID-based encryption for route discovery.

An integrated detection model was developed in [7] cluster-based wireless sensor network for increasing detection rate and reducing false rate. In [8], the classification methods are developed for intrusion detection for MANETs. The datasets cover various attack types, levels of network mobility and several data collection intervals for the intrusion detection system.

An intrusion detection and adaptive response mechanism was developed in [9] for identifying a range of attacks and provides an effective response in MANETs. An effective intrusion-detection system [10] named as EAACK particularly developed for MANETs obtains higher malicious-behavior-detection. However, the network overhead was not reduced to a required level.

An Adaptive Three Acknowledgements (A3ACKs) intrusion detection system was developed in [11] for reducing the receiver collision, restricted transmission power and attacks in MANET. A novel Intrusion Detection System was designed in [12] using the trust evaluation metrics for identifying the flooding DDOS attacks in MANET. In [13], Machine learning based intrusion detection systems for MANETs was described and it has the difficulties when constructing the topology of the network.

An intrusion detection system was designed in [14] based on *K*-nearest neighbor classification algorithm in wireless sensor network for improving the intrusion detection accuracy. Risk assessment in mobile applications have received greater attention never before with the increasing use of its applications worldwide. In [15], attacks related to mobile applications and measure for avoiding the risk assessment baseline on sensitive information and permission revocation is discussed. But, channel quality information with respect to mobile applications was not concentrated.

To analyze the performance of a base station (BS) coordination strategy, Stochastic Geometry Approach was developed in [16]. A neighbor coverage-based probabilistic rebroadcast protocol was proposed in [17], to consider the information about uncovered neighbors (UCN), connectivity metric and local node density to calculate the rebroadcast probability. Cooperation Scheme was implemented in [18] to carry out both selection combination and maximum ratio at destination in the network to improve the lifetime. The survey of several intrusion detection approaches was developed in MANET [19].A danger theory-based artificial immune algorithm was designed in [20] using mobile dendritic cell algorithm for identifying the flooding-based attacks in MANETs.

Based on the above mentioned methods and techniques, an efficient Quantum based Adaptive Topology Control (QATC) Technique is developed to increase the network transmission range and intrusion detection in MANET. The brief explanation about the intrusion detection is explained in the forth coming section.

III. QUANTUM BASED ADAPTIVE TOPOLOGY CONTROL (QATC) TECHNIQUE IN MANET

In Quantum based Adaptive Topology Control (QATC) Technique, we consider MANET be the connected path link set of 'G' with sub graphs. The connected path link graph G<V, E> where '*V*' represents the set of nodes and '*E*' represents the set of bidirectional edges. Due to the presence of intrusion, that utilize the ambiguity to carry out the malicious behavior and therefore nodes gets compromised and number of packets are not successfully received at the destinations within the transmission range. In order to overcome the above issues during transmission, the quantum based adaptive topological control technique is proposed aiming at detecting and isolating the intrusion effectively. Therefore, the packet delivery ratio is increased with minimum energy consumption.

Initially, the number of mobiles in network is grouped to form a cluster. Due to the variation in network transmission range, the number of intrusion can easily affect the network system performance. The proposed adaptive topology control technique is applied for adjusting the transmission range of the mobile nodes. This topology is also keeping the maximum number of nodes in cluster zone with minimum energy consumption. In order to achieve the intrusion detection and isolation in MANET, Quantum mechanism is applied on the cluster with minimum transmission interference.

A. Adaptive topology control technique

Adaptive topology control is used in MANET to alter the transmission range of the network. The topology control is also used to improve network wide connectivity, minimum energy and reduces interference between nodes. Initially, cluster is formed based on the intermediate nodes between the source nodes to destination. The source node is denoted as '*SN*' and destination node '*DN*'. The Neighbor Nodes exists between the source and destination pair. The entire possible neighbor nodes are grouped through which routing can be established from source to destination.

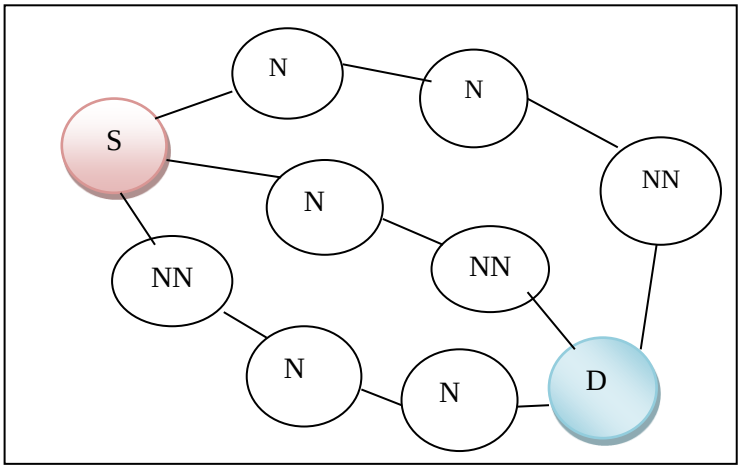

Fig-1: Formation of cluster in MANET

Fig 1 illustrates the cluster formation in MANET and complete clustering provides effective connection where the link between all the clusters contain all element pair of nodes which creates the route path. The node vertex '*V* and edges '*E*' are combined together to cluster the movable nodes of similar connected path links. The initial step uses the node with maximum degree of cluster connected path links. The application of clustering increases the broadcasting performance.

Consider a number of mobile nodes are deployed randomly throughout the network. It is assumed that all the nodes are equipped and fully connected at maximum transmission rangeTR_{max}. The objective of the Adaptive topology control is to provide a controllable and, minimal energy cost. The proposed Adaptive topology control consists of three phases such as discovery phase, topology construction phase, topology maintenance phase. At first, each mobile node determines its one-hop neighbors for establishing the route path. Mobile base station node begins the topology construction (TC) phase by transmitting a control message in second phase. Between the other nodes, the control message has information on limited neighborhood connectivity. Finally, the topology maintenance is carried out to avoid separated networks because of few control message losses.

Initially, the source node 'SN' broadcasts the control message at the maximum transmission range TR_{max}. A reliable one-hop broadcast mechanism can be used to find the one hop neighbors. This helps to reduce the possibility of undiscovered node by its neighbors.

The intermediate nodes from the source node '*SN*' within the transmission range ' TR_{max}' is measured to ensure secure routing through which data packets are

transmitted , the intermediate nodes are calculated as follows,

$$IN = \sum_{i=1}^{n} Min\left(Dis\ (SN - NN_i)\right) \quad \text{eq. (1)}$$

From eq. (1), the distances between the source node and the neighbor nodes is first evaluated. Then, based on the result obtained, the minimum distance nodes are then selected as the intermediate nodes. Based on this distance measure, the route path is selected for efficient transmission.

Step 1: Discovery phase

In discovery phase, the route is established between source and destination. The main objective is to make all the nodes receive the discovery message and formulate an entire neighbor list. After the successful reception of the control message from source node SN, the neighboring node 'NN' estimates its distance and maintains the route. The entire neighboring list is maintained and it consists of different neighbor identity and distance between the nodes. The neighbor list is then stored in ascending order.

Step 2: Topology construction (TC) phase

In proposed adaptive topology control technique, each node chooses a set of neighbors by overhearing the continuous transmission between its neighboring nodes. The neighboring node is selected to distribute its control message. Nodes that are closer to the source node are given higher priority as compared to the farther ones. The control message is also used to maintain proper value of hop distance towards the source node. As the TC phase proceeds, the control message broadcast in a limited manner such that each node communicates the control message only once. Each node maintains the following features such as Identity, backbone, hop count and neighboring list.

Step 3: Topology maintenance phase

This section describes a where the control message is lost and not successfully received at the destination. The loss of control message is major issue, because it contains information about the neighboring node. Due to this, the asymmetric routes are established where the selected neighboring node not able to extend its transmission range. Therefore, the proposed topology control technique is developed for altering the transmission range. Each node received control message from all its one-hop neighbors. Then it transmits the Request (RREQ) message at maximum transmission range TR_{max}. During the reception, only the neighboring node responds with the Reply (RREP) message. Finally, on receiving the RREP message, the source node alters its transmission range with minimum energy cost to include neighboring node by retaining the network connectivity.

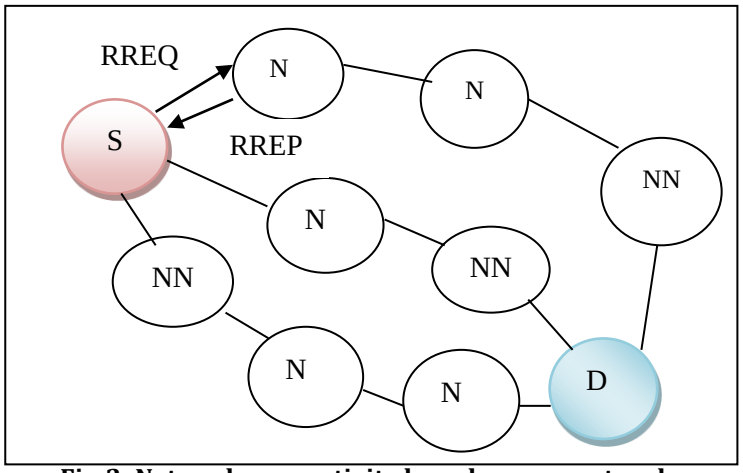

Fig-2: Network connectivity based on request and reply message

As shown in fig 2, Network connectivity based on request and reply message distribution is described in topology maintenance phase. The algorithmic description of the adaptive topology control technique is explained as below.

Input: Mobile Node '$MN_i = MN_1, MN_2, \ldots, MN_n$', Neighbor Node '$NN_i = NN_1, NN_2, \ldots, NN_n$',

$RREP$ message, $RREQ$ message

Output: Extend the transmission range of the mobile network

Begin

For each Source Node 'SN' and Destination Node 'DN'

Measure the intermediate node using minimum distance by (1)

Route Discovery phase

Step 1: obtain the information about the neighboring node

Step 2: Arrange the neighbor list in ascending order of distance

Topology construction phase

Step 3: Each node selects neighbor node to transmit a control message

Step 4: Broadcast the control message at TR_{max}

Step 5: Maintain the value of hop distance towards source node

Topology maintenance phase

Step 6: if **(**Each node received control message from all its one-hop neighbors)

Step 7: else

Step 8: Send RREQ message from SN to NN at TR_{max}

Step 9: Sends the Reply (RREP) message from NN to SN

Step 10: SN receives the RREP message

Step 12: SN extends its transmission range and improves connectivity with minimum energy cost

Step 13: end if

Step 14: end for

Step 15: end

Algorithm 1. Adaptive topology control algorithm

As shown in the above algorithm, it is adaptive to different transmission range of the mobile nodes. In discovery phase, the neighboring nodes are identified among the number of movable node in MANET for establishing the route path from source to destination. Then, the neighboring information is listed and sorted in ascending order. In second phase, topology is constructed. The topology construction control message is distributed for all the nodes at a transmission range TR_{max}. Due to this, the hop distance is maintained. In third phase, topology maintenance is performed for improving the network lifetime with minimum energy cost. This topology leaves maximum possible nodes connected in a one cluster zone with minimum energy consumption and transmission interference. As a result, it helps to increase the packet delivery ratio.

B. Quantum based secure transmission in MANET

The successful topology construction and maintenance is carried out to improve the network connectivity. Due to increasing the network transmission range, several intrusions affects the network performance. In order to reduce the intrusion in MANET, the quantum mechanism is applied for secured transmission through quantum key distribution. The application of quantum mechanism provides the sharing of a secret encryption key between the mobile nodes within the transmission range. The Intrusion Detection and isolation approach to enhance high security mobile Adhoc networks effectively detect malicious node behavior. The flow diagram of the shared key distribution is organized as shown in fig 3

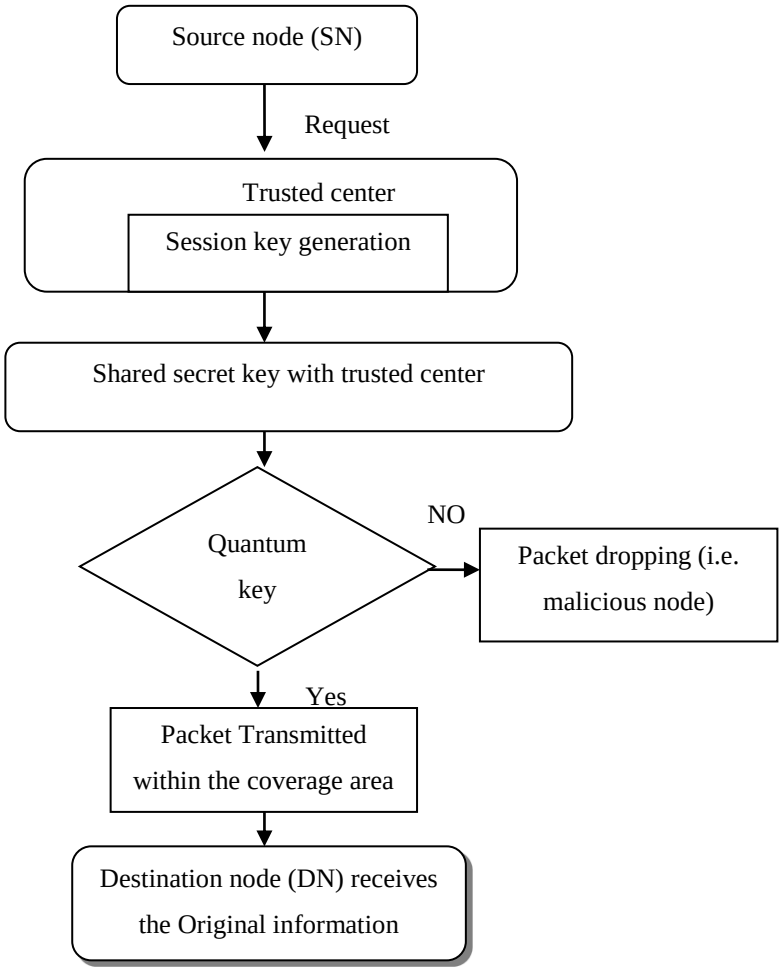

Fig 3. Flow process of quantum based key distribution

As shown in fig 3, Quantum cryptography uses quantum mechanics to enhance secure communication. It enables two parties' source node and destination to produce a shared random key to encrypt and decrypt information. An important cryptography is the ability of the nodes to detect the third party (i.e. intrusion) trying to obtain a knowledge of the key.

Quantum based key distribution depends on the principle of quantum for detecting the intrusion without disturbing the transmission. The quantum network facilitates the distribution of a secret encryption key between the nodes. The two nodes are exchanging a key with contact to achieve perfect secrecy for transmission. The ability of the source and destination to use the shared key helps to detect the intrusion. A trusted center generates a random number and a session key. It distributes the session key to the source node for encryption. Also, it distributes the same session key to the receiver side for decryption. Then the quantum key is generated using quantum information and session key. The four types of the input bit with the key value is obtained as follows,

- The input value is 0 and 0, the quantum key generate 0.707(|0> + |1>)
- The input value is 1 and 0, then 0.707(|0> - |1>)
- The value is 0 and 1, then |0>
- The value is 1 and 1, then |1>

If the shared secret key is matched with the quantum key, the transmission is performed effectively within the range. Otherwise, Packet Dropping occurs aiming at improving the security of the mobile network. This is used to detect the malicious node (i.e. intrusion) and prevents it from receiving data packets from other mobile nodes in the network.

Step 1: Malicious node isolation approach

Upon the successful detection of intrusion in MANET, the isolation is performed accordingly. The intrusion is established during the transmission packet form source to destination. A Malicious node isolation approach is used to detect the intrusion and make aware the nodes about malicious node. The source node monitors whether the data packets are transmitted or dropped by the suspected nodes If there is packet drop then the node is isolated and distributes the attack isolation message to all normal behavior nodes thus preventing further intrusion attack.

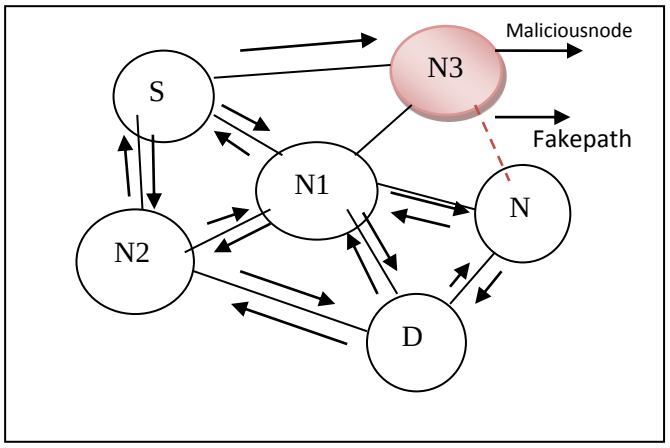

Fig 4 Malicious node behavior

In fig 4, the malicious node behavior process is described. When a node N3 is identified as the malicious node, the isolation of the node is carried out from the network. According to Malicious node isolation approach in QATC, the source node transmits an attack isolation message to inform other normal nodes in transmission range of the network. Simultaneously, the nearby nodes can receive this message. Due to this, the malicious node is isolated by removing it from the path and preventing the data packets from reaching it.

At first, the source node sends an attack isolation message to all the nodes in the network then the nodes verifies the presence of malicious node. If all nodes identify the malicious node then they detect the particular malicious path where malicious node is present. Thus the malicious node is isolated and it has fake link with other nodes in the network. After isolating the malicious node, the source node retransmits the data packets through other alternative path. For increasing the transmission, neighboring nodes do not have malicious node in routing process and also does not receive any request message from malicious node. Followed by this, the malicious nodes are isolated from the network graph and rest of the network remains connected and easily identifies the packet drop. This helps to improve the network security during the packet transmission in MANET.

IV EXPERIMENTAL SETTINGS

An efficient Quantum based Adaptive Topology Control (QATC) technique is implemented in NS-2 simulator with the network range of 1500*1500 m size. The mobile network consists of 70 nodes in the network structure and uses the Random Way Point (RWM) model. The RWM uses typical number of mobile nodes for locating

the movable nodes. The dynamic changing topology uses the Ad hoc On-demand Distance Vector (AODV) routing protocol to perform the experimental work.

The node speed is varied between 2m/s and 25m/s and the mobile node pause time is varied from 0 seconds to 300 seconds. As a result, for each metric, simulation is done for seven different seed values which are taken for the result. The simulations parameters are obtained that are used in the experiments are listed in table 1.

Table-1: Parameters value

Parameter	Value
Node density	10, 20, 30, 40, 50, 60, 70
Network area	1500*1500m
Transmission range	250m
Packets	9, 18, 27, 36, 45, 54, 63
Simulation period	600s
Minimum node speed	2m/s
Maximum node speed	25m/s
Node pause time	0 – 300 seconds
Mobility model	Random Way Point
Network simulator	NS 2.34

Experiment is conducted on the factors such as packet delivery ratio, malicious behavior detection rate, energy consumption, time to identify the intrusion. These, parameters result percentage of the QATC technique is compared against the existing intrusion detection techniques including SIEVE technique [1] and Energy-Aware Routing Algorithm [2].

V SIMULATION RESULTS AND ANALYSIS

To validate the efficiency and theoretical advantages of the proposed Quantum based Adaptive Topology Control (QATC) technique with SIEVE technique [1] and Energy-Aware Routing Algorithm [2] simulation results under NS2 are presented. The experiment is conducted on the factors such as packet delivery ratio, malicious behavior detection rate, energy consumption, and time to identify the intrusion. Performance is evaluated along with the following metrics with help of tables and graph values.

A. Impact of Packet delivery ratio

Packet delivery ratio using QATC technique is defined as the ratio of umbers of packets sent by source nodes to the number of packets successfully received at the destination nodes in MANET.

$$PDR = \frac{No.of\ packet_R}{No.of\ packet_S} * 100 \qquad \text{eq. (2)}$$

From eq.(2), packet delivery ratio PDR is $packet_R$ number of packet received, $packet_S$ No. of packet sent. It is measured in terms of percentage (%). Higher the packet delivery ratio more efficient the method is said to be.

Table 2 Tabulation for packet delivery ratio

No. of packet sent	Packet Delivery ratio (%)		
	QATC	SIEVE technique	Energy-Aware Routing Algorithms
9	91.36	85.69	81.36
18	92.74	87.37	82.98
27	93.12	88.68	84.63
36	94.63	88.97	85.74
45	95.23	89.36	85.98
54	95.69	90.10	86.25
63	96.31	91.36	87.36

The simulation values of packet delivery ratio based on the number of packet sent is illustrated in table 2. The convergence plot of seven different values is shown in chart-1.

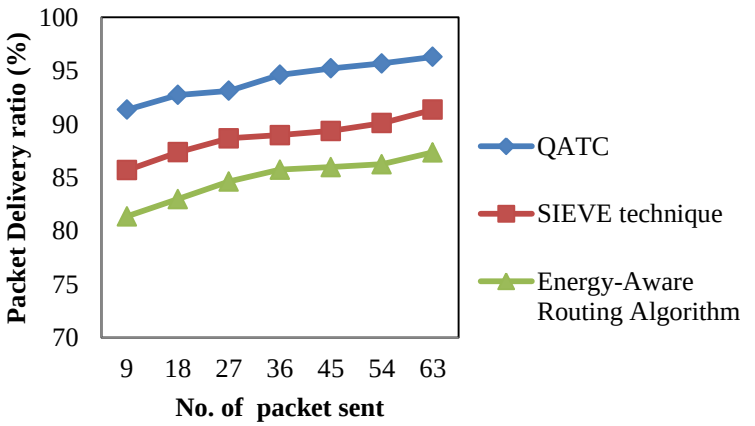

Chart-1: Measure of packet delivery ratio

Chart-1 illustrates the simulation results of packet delivery ratio with number of packet transmitted and it varies from 9 to 63. From the figure, it is clear that the proposed QATC technique achieves higher packet delivery ratio as compared to existing SIEVE technique [1] and Energy-Aware Routing Algorithm [2]. Due to this, the adaptive topology control technique is applied in proposed QATC. This topology uses the discovery phase to establish the route path by identifying the one hop neighbor. The path links are established where the selected neighboring node to extend its transmission range. This in turn improves the packet delivery ratio by 6% compared to existing SIEVE technique [1]. In addition, QATC efficiently identifies the malicious node for effective transmission. As a result, the packet delivery ratio is improved by 10% compared to Energy-Aware Routing Algorithm [2].

B. Impact of Malicious behavior detection rate

Malicious behavior detection rate in QATC technique measures the rate of malicious nodes identified in the mobile network. Due to the packet drop, malicious behavior of a node is observed. In the proposed technique, packet drop is used as a measure to detect intrusion in the network and is mathematically formulated as given below.

$$MBDR = \frac{Detect \ \ dropped \ packet}{total \ no.of \ node} \qquad \text{eq. (3)}$$

From eq.(3), the malicious behavior detection rate '$MBDR$' is observed which is ratio of detecting the number of dropped packet to the total number of nodes in MANET.

Table 3 Tabulation for Malicious behavior detection rate

No. of mobile nodes	Malicious behavior detection rate (%)		
	QATC	SIEVE technique	Energy-Aware Routing Algorithm
10	78.35	64.36	61.35
20	81.24	68.24	65.65
30	82.36	73.31	70.36
40	84.67	75.36	73.52
50	85.34	79.24	76.34
60	88.74	80.32	78.69
70	90.32	81.36	79.67

The malicious behavior detection rate using QATC technique is evaluated with two different methods SIEVE technique [1] and Energy-Aware Routing Algorithm [2] as shown in table 3. The simulation results of three different techniques are illustrated in Chart-2.

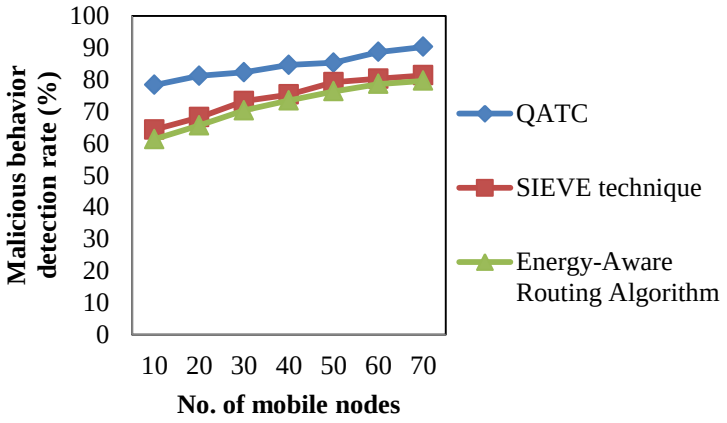

Chart-2: Measure of Malicious behavior detection rate

Chart 2 depicts the simulation of malicious behavior detection rate with respect to number of mobile nodes in MANET. The figure illustrates, our proposed QATC technique improved the performance of malicious behavior detection rate than the other state-of-art-methods [1] [2]. This is because, the malicious behavior detection rate in the QATC technique is made by detecting the malicious node using Quantum based key distribution, based on the principle of quantum. By using this key distribution mechanism, the intrusions are effectively detected without disturbing the transmission. So the performance of the proposed QATC technique is improved and increases the malicious behavior detection rate by 24% and 29% compared to SIEVE technique [1] and Energy-Aware Routing Algorithm [2] respectively.

C. Impact of energy consumption

Energy consumption using QATC technique method is the product of number of mobile nodes, power (in terms of watts) and time (in terms of seconds). The energy consumption is measured in terms of Joules (J). The mathematical formulation for energy consumption used is expressed as follows,

$$EC = No.of\ nodes * Power * Time \quad \text{eq. (4)}$$

'EC' is the energy consumption where the energy consumed by mobile nodes to reach destination.

Table 4 Tabulation for Energy consumption

No. of nodes	Energy consumption (Joules)		
	QATC	SIEVE technique	Energy-Aware Routing Algorithm
10	26.64	38.12	32.54
20	35.30	39.33	37.58
30	38.53	41.56	40.64
40	40.13	44.27	43.32
50	41.21	47.22	45.65
60	42.14	50.12	46.54
70	44.22	51.58	48.24

The energy consumption of proposed QATC technique and SIEVE technique [1] and Energy-Aware Routing Algorithm [2] are described in table 4. The comparison results of three different methods are illustrates the following chart 3.

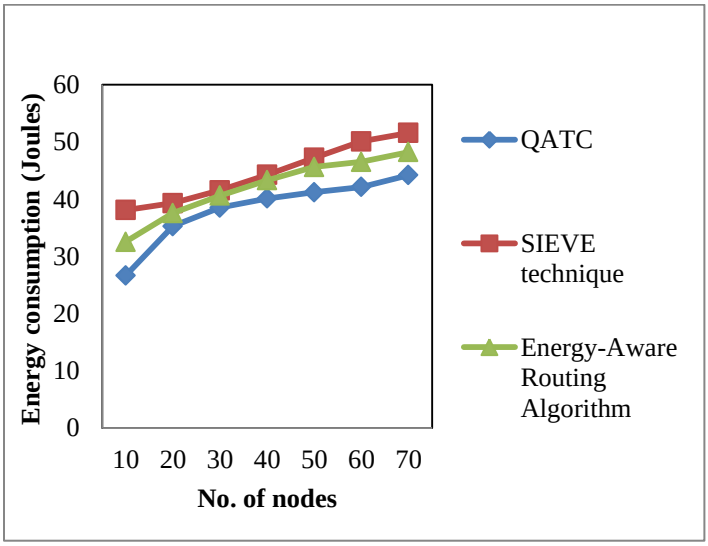

Chart-3: Measure of Energy consumption The energy consumption based on different mobile nodes with three different methods QATC technique, SIEVE technique [1] and Energy-Aware Routing Algorithm [2] performed is extensively shown in figure 7. As illustrated in figure 7, while increasing the number of mobile nodes in MANET, the energy consumption is increased in all the three methods but comparatively it is reduced in QATC technique. In QATC technique, the clustering is performed on the mobile node, then the routing path is selected for efficient transmission with minimum energy consumption. In addition, by applying topology control technique, the topology maintenance phase is carried out to improve the network connectivity. This topology will leave maximum possible nodes connected in a cluster zone with minimum possible energy consumption and transmission interference. Therefore the energy consumption is reduced by 18 % compared to SIEVE technique [1] and 10% compared to Energy-Aware Routing Algorithm [2] respectively.

D.Impact of time to identify the Malicious node

The time to identify the black hole node is measured using the number of node and the time taken to identify packet dropping during the packet transmission in MANET. The mathematical formulation for time is as given below.

$T_{MN} = No.of\ node * Time\ (Identifying\ malicious\ node)$ eq.(5)

From eq.5, where T_{MN} time to identify the malicious node, which is measured in terms of milliseconds (ms).

Table 5 Tabulation for Time to identify the malicious node

No. of node	Time to identify the malicious node (ms)		
	QATC	SIEVE technique	Energy-Aware Routing Algorithm
10	1.17	1.56	1.24
20	1.25	1.63	1.55
30	1.79	2.14	1.97
40	1.95	2.63	2.45
50	2.74	3.12	2.99
60	3.31	4.25	3.87
70	4.22	4.68	4.55

As shown in table 5, the analysis of malicious node identification time based on the number of node ranges from 10 to 70. The results of malicious node identification time using QATC technique, SIEVE technique [1] and Energy-Aware Routing Algorithm [2] is shown in chart 4.

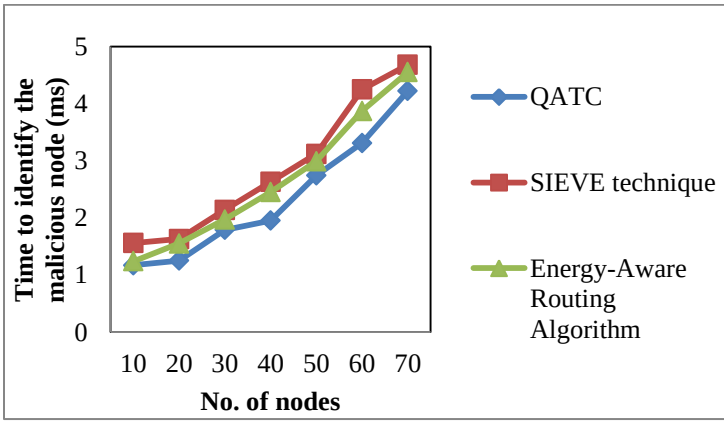

Chart-4: Measure of Time to identify the malicious node

Chart 4 reveals the simulation results of time to identify the malicious node with respect to number of mobile node in MANET. The figure illustrates, our proposed QATC technique improves the performance by reducing the time taken to identify the malicious node than the other state-of-art- methods [1] [2]. Due to this, the quantum based shared key distribution effectively identifies the malicious node to enhance secure communication. It enables two parties' source node and destination node to use shared random key to encrypt and decrypt information. Quantum based key distribution is used to detect the intrusion with minimum time. The intrusion detection time is reduced by 24% and 14% compared to SIEVE technique [1] and Energy-Aware Routing Algorithm [2].

VI CONCLUSION

In this paper, an efficient Quantum based Adaptive Topology Control (QATC) technique is developed for detecting the intrusion and isolation in MANET. Initially, an adaptive topology control is used in three phases for adjusting the transmission range of the mobile nodes to extend the network lifetime of Adhoc networks by maintaining the network connectivity. The adaptive topology establishes the effective route path with minimum energy consumption and transmission interference. After that, Quantum mechanism is applied by using the key distribution. The quantum network facilitates the distribution of a secret key between the nodes. The two nodes are exchanging a key with contact to achieve perfect secrecy for transmission. Finally, the detected malicious nodes are isolated by removing from the path and prevents the data packets from reaching them. The simulation results also reveal that the QATC technique improves the packet delivery ratio and minimizes the energy consumption. Therefore, the QATC technique also increases the malicious behavior detection rate with minimum time compared to state-of-art methods.

VII REFERENCES

[1] Rossano Gaeta, Marco Grangetto, and Riccardo Loti," Exploiting Rateless Codes and Belief Propagation to Infer Identity of Polluters in MANET", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL.13, NO.7, JULY 2014

[2]Javad Vazifehdan, R. Venkatesha Prasad, and Ignas Niemegeers," Energy-Efficient Reliable Routing Considering Residual Energy in Wireless Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 2, FEBRUARY 2014

[3] Basant Subba, Santosh Biswas, Sushanta Karmakar., "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation", Engineering Science and Technology, an International Journal, Elsevier , 2015

[4] Aneetha Avalappampatty Sivasamy and Bose Sundan., "A Dynamic Intrusion Detection System Based on Multivariate Hotelling's T2 Statistics Approach for Network Environments", The Scientific World Journal, Hindawi Publishing Corporation, Volume 2015, Article ID 850153, 9 pages

[5] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat, "Lightweight Sybil Attack Detection in MANETs", IEEE Systems Journal, Volume 7 , Issue 2, 2013, Pages 236 – 248

[6] Sayyed Musaddique, S.S.Hippargi, Attar Shuaib, "Advanced Secure Intrusion Detection System for MANET", International journal of innovative research in electrical, electronics, instrumentation and control engineering, vol. 3, issue 12, December 2015

[7] Xuemei Sun, Bo Yan, Xinzhong Zhang, Chuitian Rong., "An Integrated Intrusion Detection Model of Cluster-Based Wireless Sensor Network", Plos one journal, 2015

[8] Aikaterini Mitrokotsa, Christos Dimitrakakis, "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection", Ad Hoc Networks, Elsevier, Volume 11, 2013, pages 226–237

[9] Adnan Nadeem ,Michael P. Howarth, "An intrusion detection & adaptive response mechanism for MANETs", Ad Hoc Networks, Elsevier, volume 13, 2014, Pages 368–380

[10] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE transactions on industrial electronics, VOL. 60, NO. 3, MARCH 2013

[11] Tarek Sheltami , Abdulsalam Basabaa ,Elhadi Shakshuki, "A3ACKs: adaptive three acknowledgments intrusion detection system for MANETs", Journal of Ambient Intelligence and Humanized Computing, Springer , August 2014, Volume 5, Issue 4, pp 611-620

[12] M. Poongodi and S. Bose, "A Novel Intrusion Detection System Based on Trust Evaluation to Defend Against DDoS Attack in MANET", Arabian Journal for Science and Engineering, Springer, December 2015, Volume 40, Issue 12, pp 3583-3594

[13] Lediona Nishani and Marenglen Biba, "Machine learning for intrusion detection in MANET: a state-of-the-art survey", Journal of Intelligent Information Systems, Springer, April 2016, Volume 46, Issue 2, pp 391-407

[14] Wenchao Li, Ping Yi, Yue Wu, Li Pan, and Jianhua Li., "A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network", Journal of Electrical and Computer Engineering, Hindawi Publishing Corporation, Vol. 2014, Article ID 240217, pp.1-8,2014

[15] Yiming Jing, Gail-Joon Ahn, Ziming Zhao and Hongxin Hu," Towards Automated Risk Assessment and Mitigation of Mobile Applications", IEEE Transactions on Dependable and Secure Computing, Volume:PP , Issue: 99, Oct 2014

[16] Namyoon Lee, David Morales-Jimenez, Angel Lozano, and Robert W. Heath," Spectral Efficiency of Dynamic Coordinated Beam forming: A Stochastic Geometry Approach", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 14, NO. 1, JANUARY 2015

[17]Xin Ming Zhang, En Bo Wang, Jing Jing Xia, and Dan Keun Sung, " A Neighbor Coverage-Based Probabilistic Rebroadcast for Reducing Routing Overhead in Mobile Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 3, MARCH 2013

[18] Yong Zhou, and Weihua Zhuang, "Throughput Analysis of Cooperative Communication in Wireless Ad Hoc Networks with Frequency Reuse", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 14, NO. 1, JANUARY 2015

[19] Ehsan Amiria, Hassan Keshavarz, Hossein Heidari, Esmaeil Mohamadi, Hossein Moradzadeh, "Intrusion Detection Systems in MANET: A Review", Procedia - Social and Behavioral Sciences , Elsevier, volume 129 ,2014, 453 – 459

[20] Maha Abdelhaq, Raed Alsaqour, Shawkat Abdelhaq, "Securing Mobile Ad Hoc Networks Using Danger Theory-Based Artificial Immune Algorithm", plos one journal, May 6, 2015