International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Progressive Design of MANET Security Protocol for Reliable and Secure Communication

Mohan Patsariya[#1], Anand Rajavat[*2]

Submitted: 17/10/2023 **Revised**: 06/12/2023 **Accepted**: 17/12/2023

Abstract: The Mobile Ad-hoc Network (MANET) is a popular small area network, and rapidly deployable technology. That can be used in various applications due to flexibility, mobility, and wireless communication ability for commercial, defence, and domestic purpose. But the communication units are constrained with the resources such as battery life and security. Therefore, in this paper, we are exploring the MANET for accomplishing a secure and efficient routing. The proposed work contributes in three fields (1) providing a review for MANET routing (2) introduced a node capability based routing (NC-AODV) for improving communication reliability which contains the node quality of service for providing a capable route. (3) Introduced a Trusted node capability based routing (TNC-AODV) technique which is tested on the three security threats namely Black-hole, wormhole, and DOS flooding attack. We can also involve more attacks by incorporating the features of the attack. The implementation of the proposed technique has been carried out using NS2 simulator. Additionally, the performance of the protocol in different scenarios has been presented. The experimental results demonstrate the trust based model providing the effective security against considered attacks. Additionally, the scheme is able to improve the communication reliability in terms of Packet Delivery Ratio (PDR), and throughput. Finally, the possible and feasible future extension of the work has also been proposed.

Keywords*: MANET, security, communication reliability, node capability, Trust management, Secure routing.*

1. Introduction

The mobile ad-hoc network is frequently abbreviated as MANET. As per their name, the MANET is fully ad-hoc in nature and built with the dynamically changing network topology which is created by mobile nodes. There is not any centralized control available thus the different network activity is the responsibility of network nodes. However, the network nodes are having limited communication range thus a large but limited range of communication is performed by using the intermediate nodes, therefore, each node is acting as a router.

In order to establish communication, the source router (who wants to initiate communication) has initiated the route discovery, when the destination router is informed, then the temporary route has been established between the source and destination routers for communication. In any case, when the route has become damaged then the source or intermediate router tries to repair the route otherwise the route is again discovered by the source router. Therefore the network is highly variable and communication is unreliable. This frequent route discovery and establishment consumes the network resources. Thus we need some techniques for improving communication reliability.

On the other hand, there is no control over network infrastructure and network nodes. Therefore, any node can join or leave the network. This makes MANET vulnerable to security threats; because any malicious node can connect with the network and can perform abnormally activates which degrade the network performance. In this presented work we have described both the aspect of MANET for improving the capability of a network to make reliable communication and enhance the security of the network.

2. Related work

This section provides the study of recent studies and enhancements in the domain of MANET technology. The MANETs works based on best-effort data delivery but not offering the guarantee of reliable Quality of Services (QoS). Additionally current application demand is attracting researchers to ensure the quality of service. In this context, ***S. Tyagi et al [1]*** have investigated the AODV (Ad hoc On-Demand Distance Vector) routing, for their good and also negative aspects. Additionally a Reliability aware AODV is introduced. This technique is providing stabile routes. The routes are tested for End-to-End (E2E) Delay and Bandwidth to ensure QoS. According to this technique when a node moving slowly then route stability is not disturbed on the other hand if node moving faster than routing algorithm repairs the routing with neighbours.

[1].*Department of Computer Science & Engineering,*
Shri Vaishnav Vidyapeeth VishwaVidyalaya, Indore, India
mohan.patsariya@gmail.com
ORCID ID : 0000-0002-2013-3164
[2] *Department of Computer Science & Engineering,*
Shri Vaishnav Vidyapeeth VishwaVidyalaya, Indore, India
anandrajavat@yahoo.co.in
ORCID ID : 0000-3343-7165-777X
[3] *Computer Eng., Selcuk University, Konya – 42002, TURKEY*
ORCID ID : 0000-3343-7165-777X
** Corresponding Author Email: author@email.com*

A simulation demonstrate that variant of AODV is enhancing PDR (Packet Delivery Ratio), Throughput, and E2E Delay. Similarly, ***H. Yang et al [2]*** offers a method for trust evaluation using cluster and secure key exchange. They used a hierarchical structure for reliability enhancement. The reliability demonstrates the quality of packets and packet delivery by the trusted node. The data integrity is improved. Anomaly nodes are identified by checking DSN. Under attack, the technique can maintain performance. The performance was confirmed.

L. R. Raju et al [3] for securing and QoS routing a Node Activity-based Trust and Reputation estimation (NA-TRE) was proposed. NA-TRE concentrated on reputation and trust estimation. This technique tracks the changes in terms of packet drop or forwards for finding the node's status. The status of a node is described as Normal State (NS), Resource Limitation State (RS), and Malicious State (MS). This method is contrasted with FACE, AODV and TMS. The result shows that enhancement on throughput is 20%, 10% reduction in overhead and E2E delay. Additionally, ***D. A. Kumar et al [4]***, a Hybrid Secure Aware Routing Protocol (HSARP) is proposed to balance security and power. First, multicast routes discovery is performed. Next, the power distribution is used to enhance energy efficiency. Third, secret-sharing is used based on trust. HSRP provides better performance.

In MANETs, mobility, congestion, and link quality are crucial for path reliability. The mobility and randomness cause congestion and instability. Therefore, ***V. Tilwari et al [5]*** is proposing Mobility, Contention window, and Link quality sensitive multipath Routing (MCLMR). In order to select intermediate nodes for the route, they consider the nodes mobility, contention window, and link quality. A multi criteria technique compute weights based on mobility, window size, and link quality, additionally probable Transmissions is used reduce control message. The results show the MCLMR is superior then Multipath OLSR and MP-OLSRv2.

In various recent works the network performance is estimated using Euclidean distance. The different routes are used for communicating signal and in this situation the signal strength decreases. ***B. V. S. Kumar et al [6]*** proposed to measure the connectivity using the two ray ground, which is used in network evaluation. The results show that the reliability of a homogeneous MANET reduces. However the dependability values are less, the organization is as yet solid and it gives a plan to send the MANET. ***B. Safdar et al [7]*** modified the AODV to increase the performance. They used the ns3 to simulate AODV, DSDV, OLSR, and advanced AODV. It is noteworthy that EAODV routing performs better than OLSR. In addition, they proposed an energy-efficient model using AODV. The EAODV's is 3% superior then others.

Due to the dynamism of topology, quality of service (QoS) requirement and security MANET is a challenging. The available solutions for this context are only effective for a particular attack or expensive for QoS. ***M. S. Pathan et al [8]*** propose a trust-based secure QoS routing. The method is mitigating those nodes which are demonstrating misbehaviour in packets forwarding and ensures reliable communication. The aim is to identify appropriate node relay on capability in terms of channel quality, energy remains, link quality, etc. They demonstrate a model for the packet-dropping attack. NS2 based Simulations under different conditions show that hybrid techniques based on social and QoS trust can enhance security and QoS. ***M. G. vaighan et al [9],*** describe a stable and reliable multi-path QoS multicast routing (SR-MQMR). This method first uses the signal strength to choose the nodes. Then, route termination time and hops are used to select a route. The SR-MQMR used fewer time, decreased overhead, decreased consumed bandwidth, and increase lifetime.

Routing overhead in MANET is managed by creating multiple paths. In this condition, when a route is abundant then another route can be used. In Ad hoc on-demand multipath distance vector (AOMDV), nodes may drain energy earlier and causes link failure and required to re-establish the route. In place of reacting on link failure, a node monitors the signal strength and work accordingly. ***M. B. Dsouza et al [10]*** offers a reliable energy and link (REL). Simulation demonstrates that, REL-AOMDV has a low E2E and overhead. Similarly, ***D. H. Cho et al [11]*** design probabilistic models for MANET. This model is categorizing the moving nodes and the distance. Using simulation it was evaluated against random mobility. The authors verified this model for network life. This model is providing solution for limitations of the random mobility model by providing better energy efficiency and stability. According to ***D. Sinwar et al [12]*** the optimized path has utilized Swarm Intelligence such as Ant-Colony Optimization (ACO), Particle Swarm Optimization (PSO). By applying ACO routing provides the improved PDR, throughput, less energy consumption and E2E delay. They compare the protocols namely AODV, AOMDV, DSDV, and ACOP using Random Waypoint Model. Performance is including PDR, Throughput, and E2E Delay.

To make the Internet of things (IoT) a reality, more attractive, and economic. ***W. Alnumay et al [13]*** discuss a trust model which includes direct and indirect trust. Both the trust is combined by Beta probabilistic distribution. The ARMA/GARCH has been used for combining the trust evidence and predicts trust. Finally a routing is developed for secure and reliable E2E delivery. Similarly, ***V. S. Ingle et al [14]*** proposed a composite trust metric using social trust and QoS. That is implemented on AODV

protocol with an attack identification method for handling the adversary's packet-forwarding misbehaviours. They present working of three attack models. Results show that the social and QoS trust offers an enhancement on PDR, energy used and routing overhead.

M. Ponguwala et al [15] offers a method to secure MANET-IoT. They propose a cluster-based technique with recommendations. The ML algorithm is used for recommendation. The network is clustered using the Secure Certificate-based Group Formation (SCGF) process. The K-means is used to compute trust. In order to provide secure route a hybrid algorithm is proposed using the Genetic and FireFly Algorithm (GA-FFA). Data is secured using a Hash Message Authentication Code with AES (HMAC-AES) and cryptography. The simulation in NS-3 has been done and found better outcomes. ***Dr. S. Ramesh et al [16]*** used Protected Reliable Routing (PRR) for security. Node formation is performed by two way secured encrypted that cross-validate for false node in case of multicast communication and MD5 and HMAC is used for unicast communication. Bee's algorithm is used to avoid delay, based on the higher objective value and then source node. The efficiency of PRR is shown by comparing it with existing techniques.

According to ***S. Naveena et al [17]*** black-hole is decreasing the PDR. The attacker is claimed as the best path. If attacker receives the data, all packets are dropped. Thus, a trusted routing is used for routing into two stages, first locate and secure all node communication system and second predict a safe path. ***R. Tourani et al [18]*** introduced PERSIA, for prevention and detection of DoS flooding. The attack prevention technique eliminates the attacks possibility. Under attack condition, PERSIA used to handle attack's consequence. Experiments show PERSIA's resiliency and effectiveness. According to ***D. Chouhan et al [19]*** software-Defined Networking (SDN) is promising in the 5G to deal with DoS and DDoS threats. They propose to detect and eliminate DoS and DDoS attacks using an entropy-based technique.

A limited solutions utilizing machine learning for detection of DOS attacks. The existing solutions are inefficient to handle these attackers. ***K. G. Reddy et al [20]*** introduced a solution to deal with DDoS attack. This method includes an authentication system and naïve Bayes algorithm for identification and removal of attack. The results show that method outperforms and secures the network.

The design of secure and energy-efficient routing is a complicated task due to limited resources. To address this complexity ***N. Veeraiah et al [21]*** offer a trust-based routing using cat slap single-player algorithm (C-SSA) to find nodes for routing. Initially, the fuzzy clustering is used to select cluster heads (CHs) with maximum worth. The CHs is also participates in routing, and the best route is calculated using a hybrid method. The routes are obtained using delay, throughput, with connectivity. According to ***R. Pandey [22]***, MANET is a spot of concentration in the correspondence framework. A collection of wormhole nodes is used for directing promotion sales systems. This attack is called a communitarian attack. A clog has been produced. Because of the delay in the packets, the control message sends by the genuine node. To deal with attacks the countermeasure which Trust esteem is figured out. The developed trusted AODV protocol is assessed which shows improvement on standard AODV.

Security issue in MANET is promising research. In 2011, ***F. H. Tseng et al [23]*** had a survey of the black hole in MANETs. They survey on Black-hole attacks published in last 5 years. The Black-hole attacks are categorized as collaborative and non-cooperative attacks. Additionally some other attacks like flooding and wormhole was discussed. Moreover, they are providing research issues and future trends for detection and prevention of attacks. They summarize detection techniques with comparisons of a non-cooperative, collaborative, and other attacks. ***M. Shukla et al [24]*** considers black hole and wormhole with two types of protocol AODV and elliptic curve cryptography. By considering wormhole as A and Black-hole as B they have prepared a function. The two more things that have been discussed are energy and overhead. The SWBAODV were superior in front of BAODV and WAODV.

3. Node Capability Based Routing (NC-AODV)

The proposed work is aimed to investigate MANET in order to offer secure and reliable communication. Therefore we have subdivided the entire efforts into two major parts first Node quality estimation based routing design and then the trust for securing the network from various different attacks. In this context first, in this section, we have discussed the node quality estimation-based routing. The node quality has been defined as the node capability. The node capability is a selection criterion of nodes in a route during the discovery of a route between sources and sink routers. Therefore the node capability is an indicator of good quality of service delivering routers in the network. In this context to find the capable routers in the network, we have considered the different quality of service parameters as:

a. **Energy:** In MANET energy is one of the critical resources for the mobile node. The low power node can behave abnormally and can negatively affect the performance of the network. Therefore we need to identify the energy resourceful nodes for developing the communication routes. In this work, we use the energy parameter as **E.**

b. **Buffer length:** buffers are used as the small storage

unit for communication data, during the sending, receiving, and forwarding. The less size of the free buffer can create performance degradation by congestion or information loss. Thus we need a considerable buffer length for efficient communication, which is denoted here as **B.**

c. **Mobility:** the mobility of nodes has also impacted the performance of the network performance. The highly mobile node cannot be reliable due to frequent path breaks. Thus less mobility of nodes is beneficial for the network. That is denoted here as **M.**

d. **Available bandwidth:** the nodes are communicating with each other efficiently when sufficient bandwidth has available. Thus in order to include the link quality during the communication, we include the link quality parameter as bandwidth which is denoted here as **AB.**

The considered quality of service parameters is used for selecting the suitable and capable nodes for the formation of effective routes. Figure 1 and Figure 2 demonstrate the steps of routing based on the node capability-based routing strategy. The routing strategy has been implemented on the AODV routing protocol. Thus, the source start route discovery by Route Request (RREQ) packet broadcast. In response, the reverse route has been created. Traditionally in AODV as the reverse route has been created the communication has started. But in the proposed work we have modified the protocol to wait for receiving replies from all its neighbours. After getting replies from the neighbours' protocol start evaluation of routes has been initiated. During the evaluation, the node's quality of service values of energy, buffer length, mobility, and the available bandwidth is calculated for all the intermediate nodes. However, these values are calculated on different scales therefore first we need to normalize these values into a common scale. Thus we use the min-max normalization to scale the QoS values between 0 to 1. The following equation can be used for normalizing the values.

$$NormValue = \frac{val - min}{max - min}$$

Now, after normalization of the values, we have calculated the threshold for node capability. In this context, we use the mean of all node values of quality of service. The following equation can be used for this task.

$$T_c = \frac{1}{N}\sum_{i=1}^{N}\frac{B_i + E_i + M_i + AB_i}{4}$$

This calculated threshold has been used for classifying the node capability. If the node's capability threshold T_i is higher than the overall threshold's T_c 75% then we have classified the node as a capable node otherwise we consider the node is less capable. If the node is capable then we label the node as 1 otherwise the node label becomes 0. After labelling all the nodes we need to rank the routes.

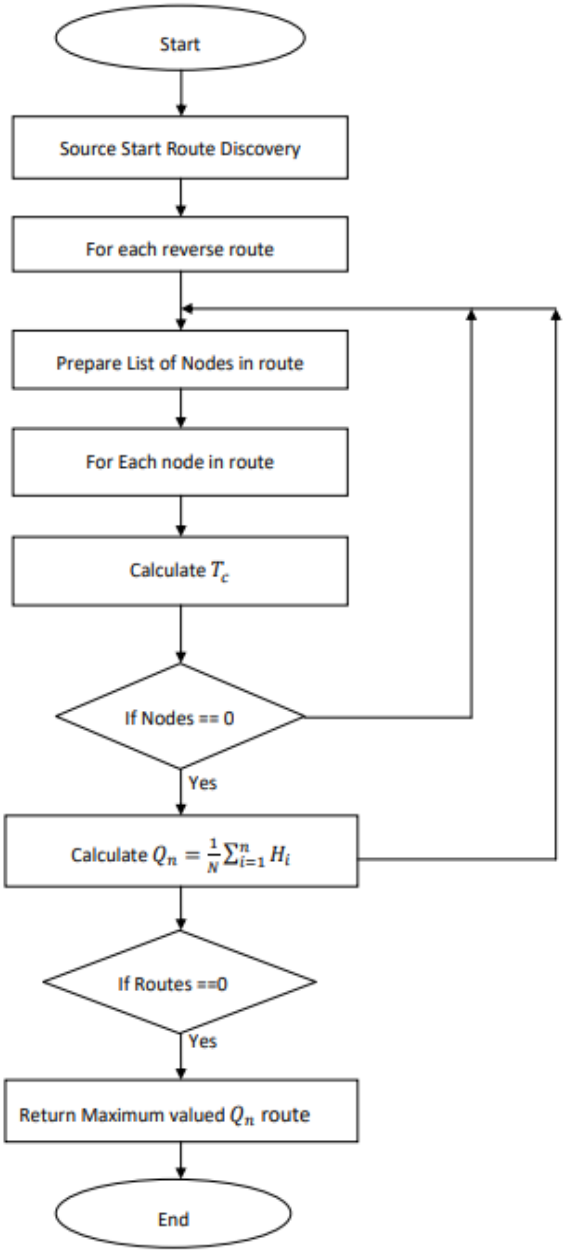

Fig. 1 Flow chart for node capability based routing

The rank is given on the basis of the entire route's quality of service. Thus the route which contains most of the nodes as capable is selected for the communication. Thus in order to calculate the route rank, the following equation will be used:

$$Q_r = \frac{1}{M}\sum_{i=1}^{M} H_i$$

Where the M is number of hops in the route, H_i is the i[th] node. capability, and Q_r is the route capability rank

Finally after calculating route capability we have selecting the most higher ranked capable route for reliable communication. The described concept of route selection based on node capability has implemented using the AODV routing protocol in NS2 simulation technology. Additionally the performance of the routing has been measured in different performance parameters. Additionally the comparison with the classical AODV routing has also been performed. In this context, first, we have measured the end-to-end delay of routing.

Input: Number of routes to be evaluated (N)

Process:

1. Source S initiate route discovery
2. for each reverse route to destination
3. $R_n = Select\_Top\_Routes(N)$
4. $for(i = 1; i < N; i++)$
   a. $H_m = getHop(R_i)$
   b. $for(j = 1; j < m; j++)$
      i. $M = getMobility(H_j)$
      ii. $B = getBuffer(H_j)$
      iii. $E = getEnergy(H_j)$
      iv. $AB = getBandwidth(S, H_j)$
      v. $T_c = \frac{M+B+E+AB}{4}$
      vi. $if(T_c > 0.75)$
         1. $H_j = 1$
      vii. Else
         1. $H_j = 0$
      viii. End if
      ix. $H_i = H_i + H_j$
   c. $endfor$
   d. $Q_n = \frac{1}{N}\sum_{i=1}^{n} H_i$
5. $endfor$
6. $index = getMax(Q_n)$
7. $R = R_{index}$
8. $returnR$

Fig 2. Algorithm for NC-AODV

The E2E delay is measured here in terms of milliseconds (MS). Figure 3(A) shows the comparative E2E delay of AODV and Node Capability-based AODV (NC-AODV). The E2E delay is the amount of time required for communicating a packet source to sink. According to the obtained E2E delay of both the routing techniques we can see the E2E delay of the proposed NC-AODV routing is low as compared to the AODV routing technique due to efficiency and utilization of higher bandwidth. Thus the NC-AODV is suitable for good and reliable communication

Similarly, we have measured the energy consumption of the network nodes. The energy consumption of the different network sizes is demonstrated in figure 3(B). The network nodes are utilizing energy from their initial energy level for different network events. Thus energy is a critical resource for MANET. The low energy consumption is beneficial for a good network routing technology. According to the measured energy consumption of both NC-AODV and classical AODV, we have found the proposed NC-AODV routing provides low energy consumption compared to the AODV routing. So, the given model will be helpful in preserving the energy for normal communication scenarios. The next parameter is the routing overhead, which is the amount of total additional control messages exchanged during the communication scenarios. The routing overhead for both methods is shown in figure 3(C). The experiments show that increasing network size will increase the routing overhead in different communication scenarios. Additionally, we have found that the NC-AODV and AODV demonstrate a similar overhead but the quantity of NC-AODV routing's overhead is less as compared to the AODV routing technique. Figure 3(D) demonstrates the PDR, which is need to e higher for better communication. That is the number of packets conveyed to the sink node. Here the PDR is calculated in terms of percentage (%). According to the results obtained the PDR of NC-AODV is significantly higher as compared to AODV protocol. Similarly, the mean throughput of both the network configurations is described in figure 3. The throughput is an indicator of bandwidth utilization. The higher bandwidth utilization is the ability to deliver a higher rate of data transfer. That is become feasible due to all the nodes in the route are efficient and capable to communicate. Thus the proposed NC-AODV routing is providing higher throughput as compared to the classical AODV routing.

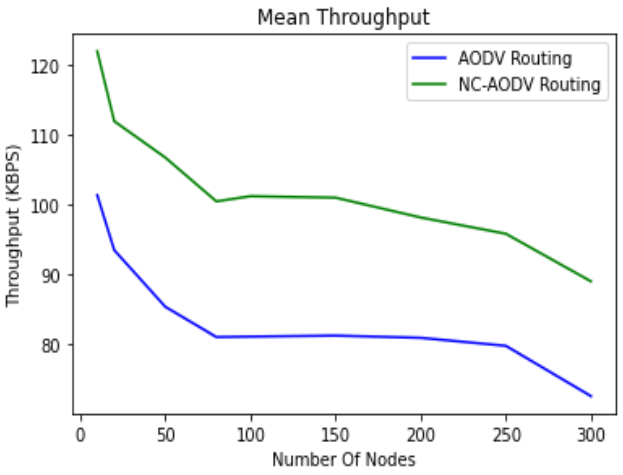

Fig 3 Throughput analysis AODV Vs NC-AODV

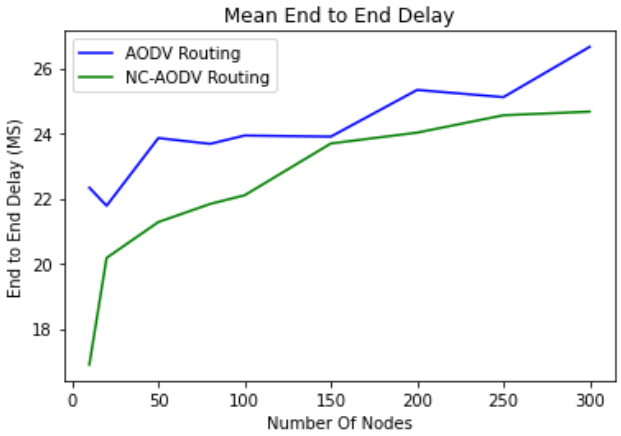

Fig:3(A) E2E Delay analysis AODV Vs NC-AODV

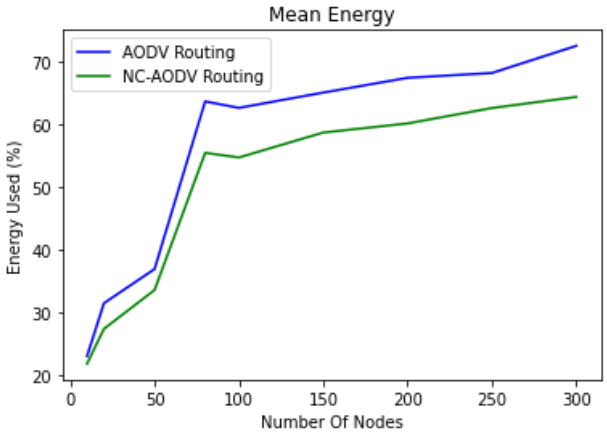

Fig:3(B) Mean Energy consumption analysis AODV Vs NC-AODV

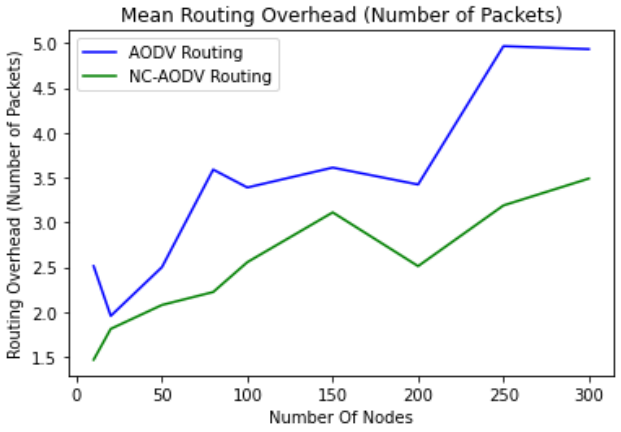

Fig:3(C) Routing overhead analysis AODV Vs NC-AODV

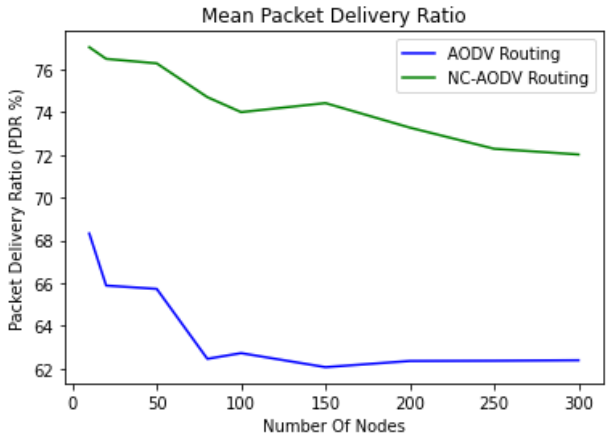

Fig:3(D) PDR analysis AODV Vs NC-AODV

Based on the different performance matrix measurements we found that the selection of good quality nodes for communication can enhance the performance in terms of energy consumption, PDR, E2E delay, and throughput. Thus the proposed method of NC-AODV is promising for more improvement and adopting the security concepts to offer secure and reliable communication in the network. This section describes the functional and experimental observations of the proposed routing technique NC-AODV. Additionally, the next section demonstrates the working of the trust-based routing, which is an extension of the NC-AODV routing.

4. Trusted and Node Capability based Routing (TNC-AODV)

The MANET is a fully dynamic network infrastructure and due to this MANET frequently changes its topology. In addition, new nodes can also join and leave the network infrastructure according to their own needs. Therefore the network is prone to be compromised by different kinds of network attacks. Thus, aim is to extend the NC-AODV routing protocol for providing security against different network attacks. In this context, we are proposing a trust-based routing for improving network security also. The trust-based routing technique involves a trust measurement system for individual nodes as well as for the entire selected route. That minimizes the risk of compromising the network against security threats. In this context, we identify the following key parameters by which we are creating trust for validating an efficient and secure route. Thus we proposed to measure the two factors as:

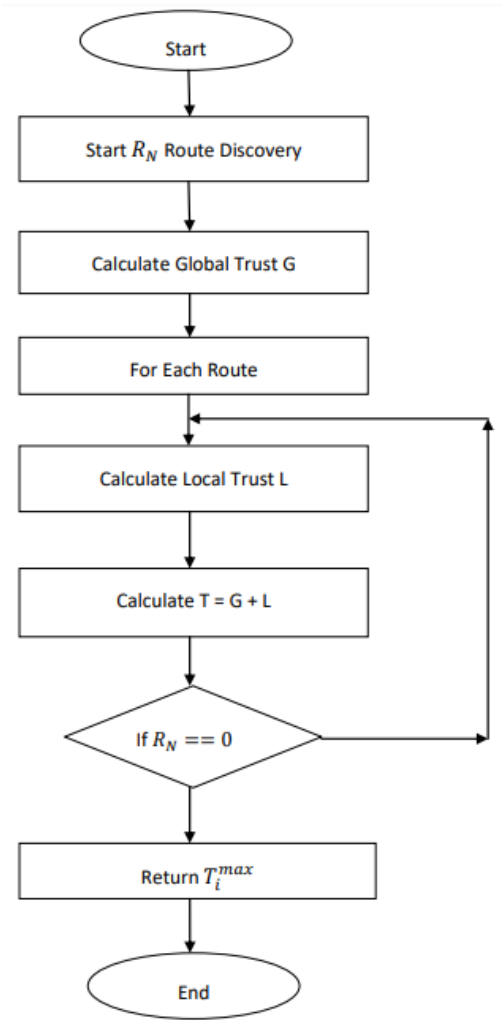

Fig 4: flow chart of Trust Based routing technique

Measuring global trust: the global trust is denoted using G, which demonstrates the historical view of the neighbors. That can also be termed as the social trust of the node, thus from three neighbors of the route nodes we are asked: "Is the previous node sent data to the neighbor". If the nodes respond with yes or in-network terms if the neighbor has the entry of the target route node then the algorithm considers it a weighted point. Thus if the response of R_i is true then we computing the global trust of the destination node as:

$$G = \frac{1}{N}\sum_{i=1}^{n} R_i$$

Where N=3 in this experiment, that can be modified according to network designer's need and need of security level requirement in the application.

Measuring local trust: that is measured on the basis of each route which is being discovered by evaluation of nodes in the discovered route/s. In order to compute the individual node's local trust the following function will be used:

$$L = \frac{E + F + P + AB}{4}$$

Where,

L = Local Trust for a node

E = Energy Remain in node if % of energy remain > 33% then E =1

F = amount of RREQ flooding is less then T_{RREQ} then F =1

P = PDR in % is > 60% then P = 1

AB = Available bandwidth in % is > 33% then AB = 1

Finally for measuring the local trust for entire route the following equation will be used:

$$L_R = \frac{1}{N}\sum_{i=1}^{N} L_i$$

Where,

N = number of nodes in route

L_i = Trust of ith node

L_R = Local Trust for the entire route

Measuring the trust of route

$$T = G + L_R$$

The steps of managing trust are demonstrated in figure 4 and figure 5.

Input: Destination D

Output: Selected secure route S

Process:

1. $R_N = Route\ Discovery\ using\ NC - AODV$
2. $G = CalculateGlobalTrust(D)$
3. $For(i = 1; i < N; i++)$
    a. $L_i = CalCulateLocalTrust(R_i)$
    b. $T_i = G + L_i$
4. $end\ for$
5. $T_i^{max} = GetMax(T_i)$
6. $S = SelectRoute(T_i^{max})$
7. $return\ S$

Figure 5: TNC-AODV Algorithm

The process has initiated after discovering the route by using the previously described routing protocol NC-AODV. That protocol will help here for establishing the initial route between source and destination. After establishing the route the destination node broadcast a message to their neighbor for demonstrating their social trust level. When the nodes are getting trust request then the nodes check their routing table for the destination node's entry.

5. Performance Analysis of AODV Vs NC-AODV Vs TNC-AODV

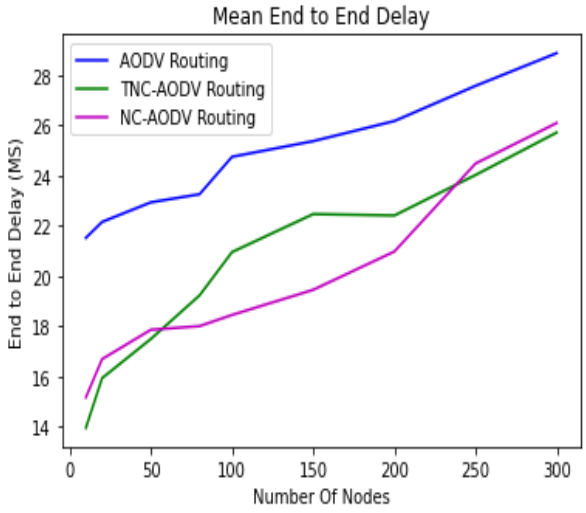

Fig 5(A): E2E analysis of AODV Vs NC-AODV Vs TNC-AODV

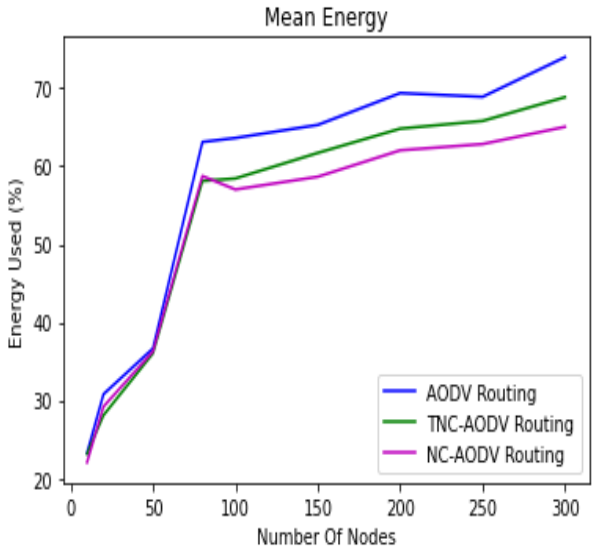

Fig 5(B): Energy Consumption analysis of AODV Vs NC-AODV Vs TNC-AODV

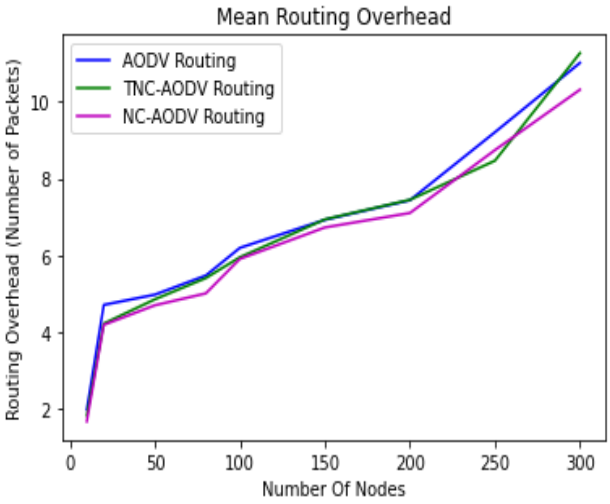

Fig 5(C): Routing overhead analysis of AODV Vs NC-AODV Vs TNC-AODV

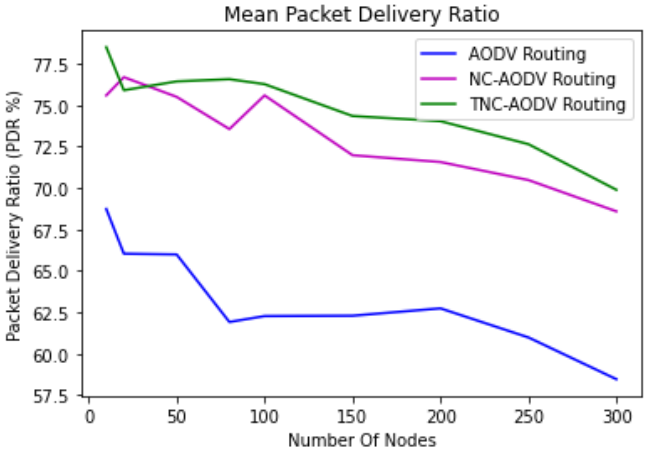

Fig 5(D): PDR analysis of AODV Vs NC-AODV Vs TNC-AODV

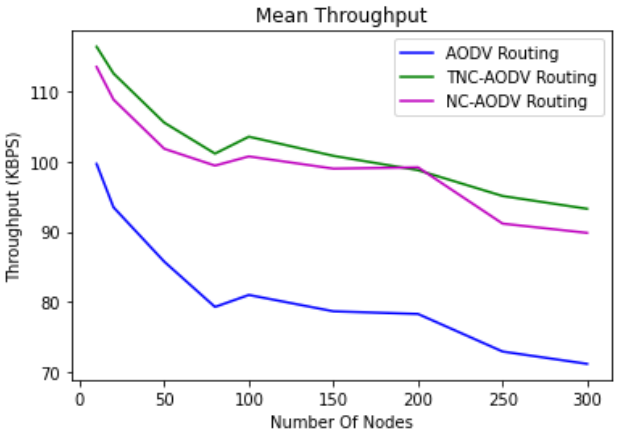

Fig 5(E): Throughput analysis of AODV Vs NC-AODV Vs TNC-AODV

If the neighbor nodes are found their entry in routing table then respond with the flag 1 otherwise send the flag to 0. Using this reply the destination of calculate the global trust and communicate to the source node. As the source node found the global trust value then start computation of local

trust value as described in equation of L_R. Based on the both of the values global and local the source node decides to start communication with the destination node. The proposed trust-based technique has been implemented on the NC-AODV routing for security to the network. In this context first, we have verified the performance of the implemented model using the normal communication scenario. Thus, we have contrasted the performance of AODV, NC-AODV, and Trust-based NC-AODV (TNC-AODV). Thus similar parameters to the previous experiment have been calculated i.e., E2E delay, routing overhead, throughput, energy consumption, and PDR. The performance of the TNC-AODV, NC-AODV and AODV are demonstrated in figures. Figure 5(A) gives the E2E delay of the network with the implemented routing protocols with different network sizes. Additionally, the mean performance has been demonstrated.

According to the obtained results in terms of end-to-end delay, the TNC-AODV demonstrates a similar E2E delay as NC-AODV but still, it slightly improved as compared to NC-AODV and largely as compared to classical AODV. Similarly, the energy consumption which is described in figure 5(B) demonstrates the TNC-AODV preserves a higher amount of energy as compared to both the other implemented versions of the AODV routing protocol. Next, we have measured the routing overhead and compared it with the AODV and NC-AODV routing protocols. The comparison of routing overhead is demonstrated in figure 5(C). According to the obtained results in terms of routing overhead, the TNC-AODV demonstrates fewer routing overhead as compared to the other two implemented routing protocols.

Next, we have measured the PDR which is given in figure 5(D) and then we described the performance of the network in terms of throughput. The throughput is given in figure 5(E). Both the parameters are demonstrating similar performance and also show a higher throughput and PDR as compared to the NC-AODV and AODV routing protocols.

This section demonstrates the performance of the network in normal network communication scenarios for all three routing protocols. The next section is describing the security analysis of the protocols under different attack scenarios

6. Performance Analysis of AODV Vs NC-AODV Vs TNC-AODV under Different Types of Attacks

The design and evaluation of trust-based NC-AODV have been described in the previous section. The experimental analysis of the TNC-AODV demonstrates the effective and improved performance as compared to NC-AODV and AODV. However, the TNC-AODV has works fine with the normal network scenario but the trust concept has been included to advance the security of the network among different kinds of attacks in the MANET. Therefore, we need to validate the TNC-AODV routing with the attack in the network. In this context, three crucial MANET attacks have been considered namely Black-hole attack, wormhole attack, and DOS flooding attack. The overview and effect of these attacks under different network configurations have been described in this section.

Black-hole Attack: the Black-hole attack is a most crucial attack in MANET. Here, the attacker has trying to eliminate the communicated packets between source and destination. The attack is deployed when the normal routing protocols are initiating the route discovery.

During the route discovery when the source node start the flooding of RREQ packets and malicious node found the request message then the malicious node keep the RREQ message and a false Route reply message (RREP) has created. This false RREP message is communicated to source node. The destination node when get the route reply then start communication by using the attacker node. The attacker node then drops all the communicated packets from the network. In this way the Black-hole attack degrade the performance of the network.

Wormhole Attack: the wormhole attack is an effort of more than one attacker. In other terms, the wormhole attack has deployed with at least two or more attackers. In this attack two attackers are creating a high speed communication link between self. Due to this high speed link the network nodes are start communication with this link and then congestion has formed in this link. This phenomenon most of the communicated packets are dropped and network performance has been negatively affected. Therefore the wormhole is a most crucial attack in MANET which influences the performance of the entire network.

DoS Flooding Attack: the DoS flooding attack is deployed to target a specific network node to disturb the node from getting network services. In this context, the attacker continuously floods the RREQ packets to the victim node. The victim node has started working on these flooded packets by the attacker and soon the victim has stopped working normally due to full of their communication buffer. The result is the victim node is not able to send or receive any packet from the network and stops working. Thus that is also a critical attack of MANET which degrades the network performance.

After introducing the considered attack of the MANET we have deployed attacks in configured networks based on protocols AODV, NC-AODV, and TNC-AODV. Additionally, the simulation of different network sizes has been carried out. After simulation, we are measuring the mean performance of the networks in terms of similar

parameters as we have described in previous experiments. The E2E delay of the networks under a Black-hole attack is demonstrated in figure 6(A). According to the obtained results, the E2E delay of the AODV based network shows near about 0 because due to the attack no data has been communicated to the sink node. On the other hand, the NC-AODV and TNC-AODV based routing protocols are demonstrating similar end-to-end delays. But as compared to NC-AODV the TNC-AODV demonstrate a low end-to-end delay for attack conditions. Additionally, when we measure the energy consumption as given in figure 6(B), the traditional AODV routing protocol shows higher energy consumption as compared to other implemented protocols additionally the TNC-AODV routing shows the minimum energy consumption.

Next when we discussed the routing overhead as reported in figure 6(C) demonstrating the similar pattern of all the implemented routing protocols. But the overhead of traditional AODV is higher than both the other implemented routing protocols. Next, we can see the PDR which is given in figure 6(D) demonstrates the higher PDR of the TNC-AODV routing protocol but the AODV routing protocol demonstrate the minimum PDR because the Black-hole is interrupting the communication and no data has been exchanged between the sources and sink router. A similar effect we can also see in performance in terms of throughput which is demonstrated in figure 6(E).

Here also the throughput of AODV routing is very fewer and. On the other hand, the NC-AODV and TNC-AODV routing can show strength against the Black-hole attack but the TNC-AODV will be able to deal better with the Black-hole attack as compared to the NC-AODV routing protocol. Next, we have applied the DOS attack and wormhole attack to the implemented networks. The performance of the network under DOS attack is given from figure 6(F) to figure 6(J). Additionally, the performance under wormhole attack is given from figure 6(K) to figure 6(O) . According to the given performance of the protocols under DOS and wormhole attacks, NC-AODV and TNC-AODV demonstrate similar behavior. According to the measured results under the considered attack conditions we can see the attack can significantly degrade the network performance configured based on the AODV routing protocol. On the other hand, the network configured based on NC-AODV has been impacted due to attacks but can survive by enabling the services and communication. But the TNC-AODV routing protocol has demonstrated the avoidance ability against the considered attacks. Thus the proposed concept of NC-AODV and TNC-AODV can improve the network performance and also can deal with network attacks with significant performance.

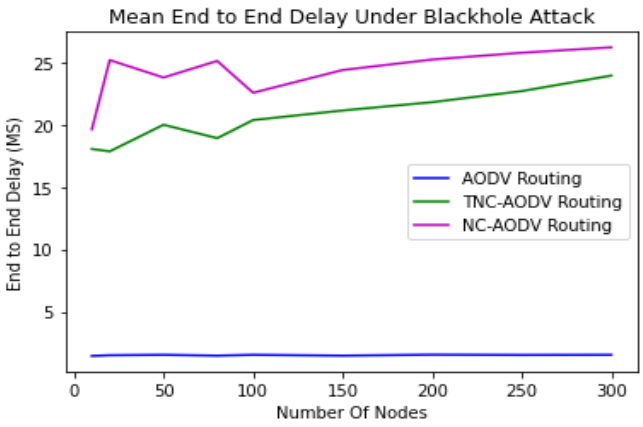

Fig 6(A): E2E analysis of AODV Vs NC-AODV Vs TNC-AODV under Black-hole attack

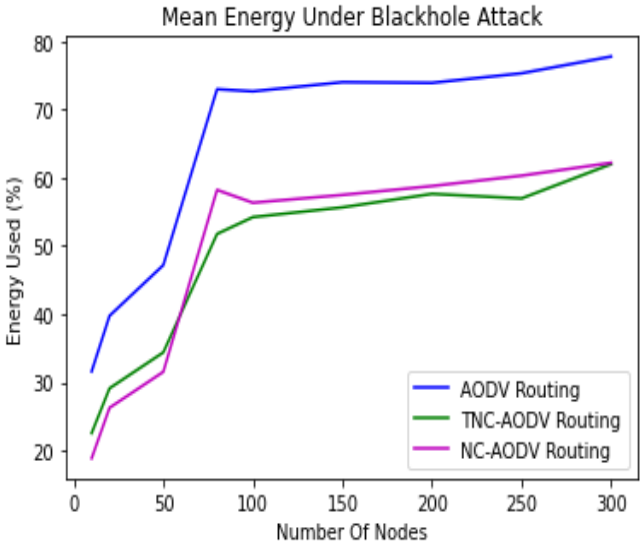

Fig 6(B): Energy consumption analysis of AODV Vs NC-AODV Vs TNC-AODV under Black-hole attack

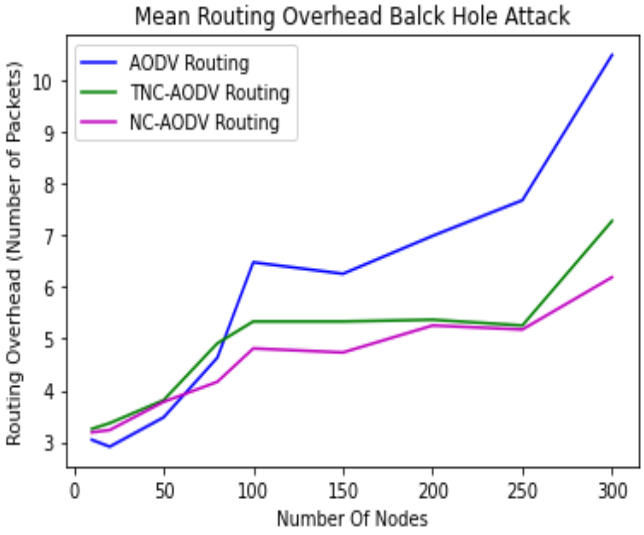

Fig 6(C): Routing Overhead analysis of AODV Vs NC-AODV Vs TNC-AODV under Black-hole attack

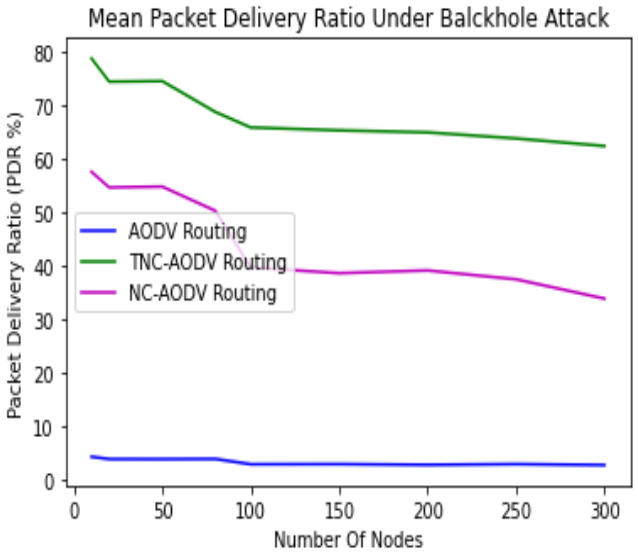

Fig 6(D): PDR analysis of AODV Vs NC-AODV Vs TNC-AODV under Black-hole attack

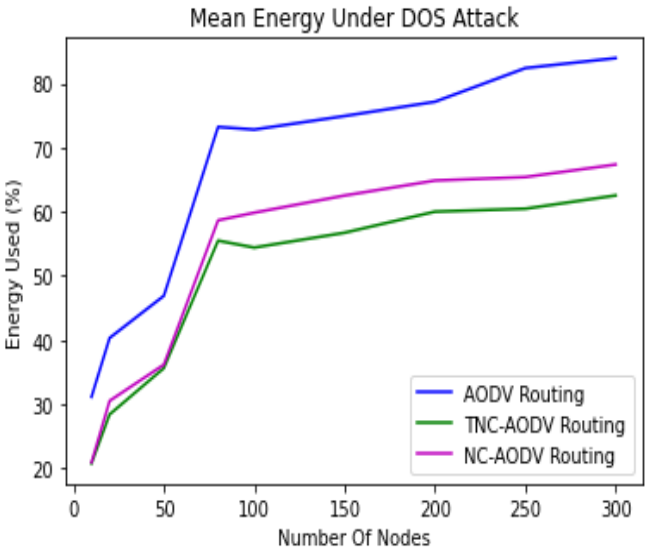

Fig 6(G): Energy consumption analysis of AODV Vs NC-AODV Vs TNC-AODV under DOS attack

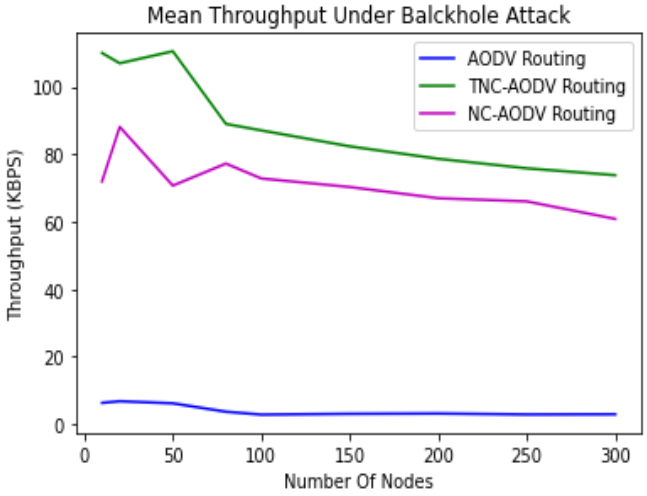

Fig 6(E): Throughput analysis of AODV Vs NC-AODV Vs TNC-AODV under Black-hole attack

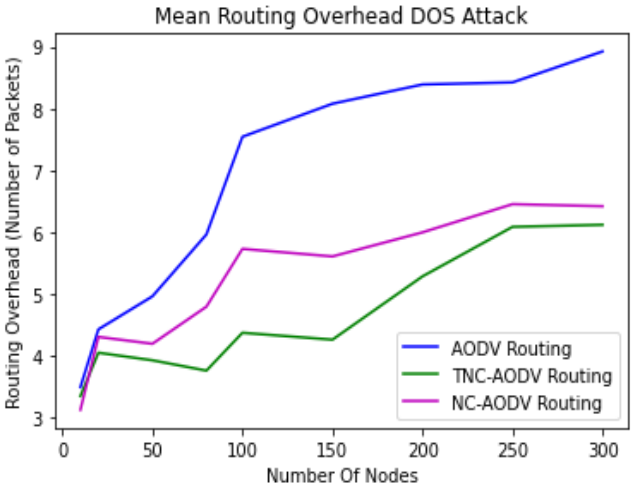

Fig 6(H): Routing overhead analysis of AODV Vs NC-AODV Vs TNC-AODV under DOS attack

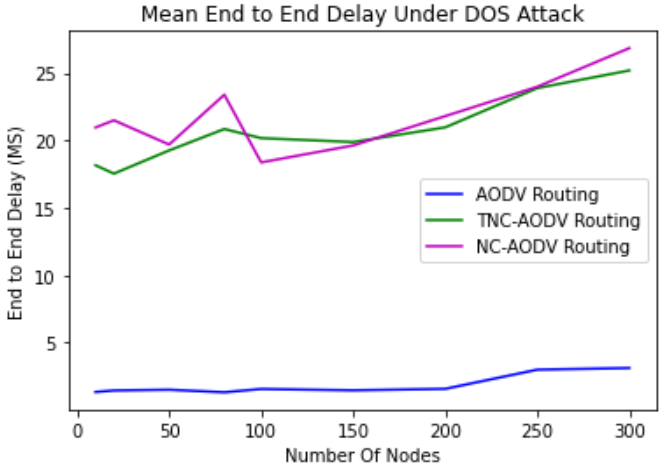

Fig 6(F): E2E analysis of AODV Vs NC-AODV Vs TNC-AODV under DOS attack

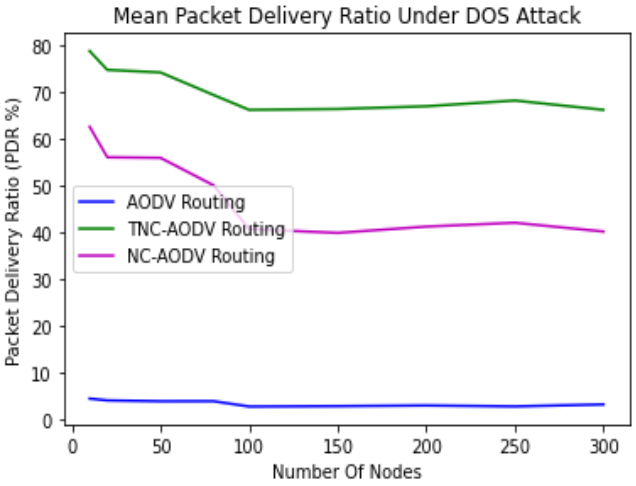

Fig 6(I): PDR analysis of AODV Vs NC-AODV Vs TNC-AODV under DOS attack

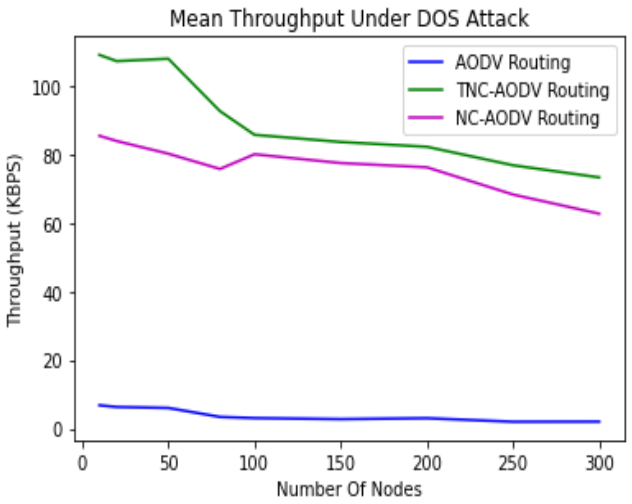

Fig 6(J): Throughput analysis of AODV Vs NC-AODV Vs TNC-AODV under DOS attack

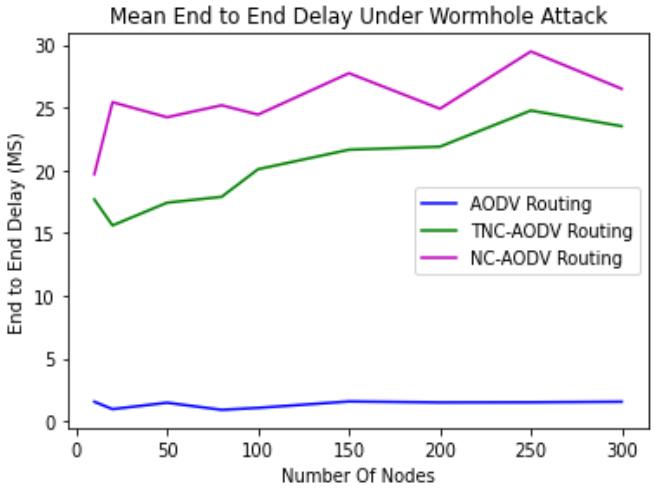

Fig 6(K): E2E analysis of AODV Vs NC-AODV Vs TNC-AODV under Wormhole attack

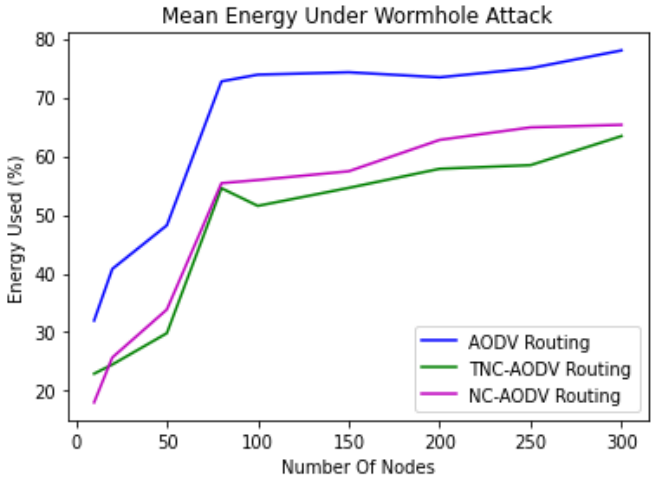

Fig 6(L): Energy concumption analysis of AODV Vs NC-AODV Vs TNC-AODV under Wormhole attack

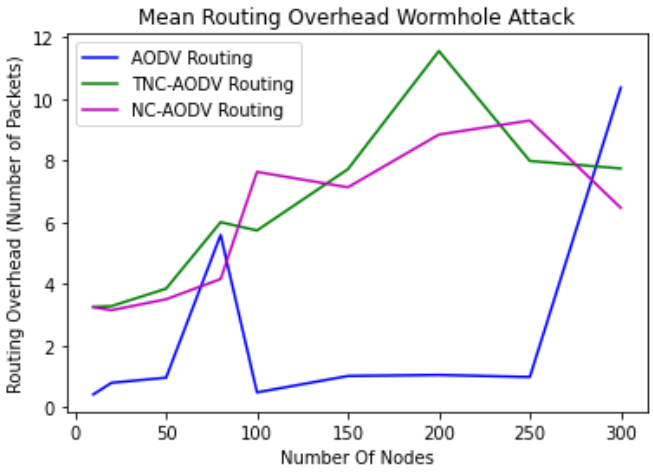

Fig 6(M): Routing overhead analysis of AODV Vs NC-AODV Vs TNC-AODV under Wormhole attack

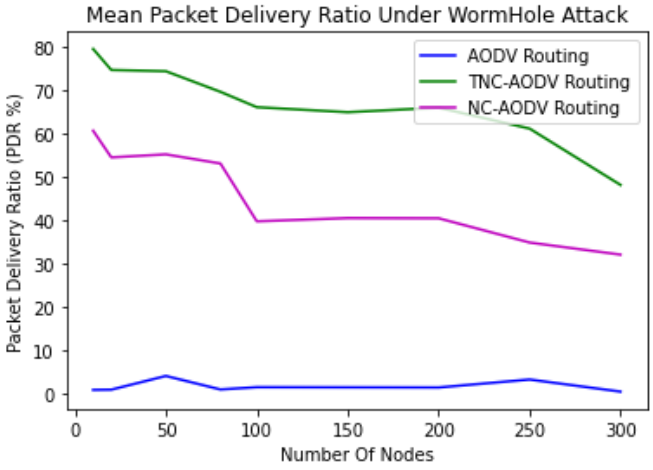

Fig 6(N): PDR analysis of AODV Vs NC-AODV Vs TNC-AODV under Wormhole attack

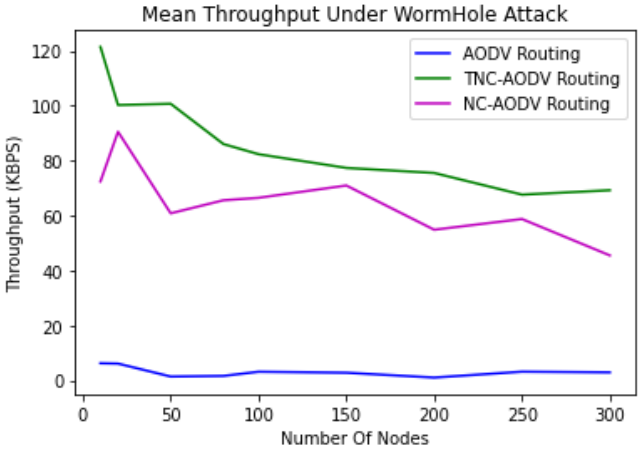

Fig 6(O): Throughput analysis of AODV Vs NC-AODV Vs TNC-AODV under Wormhole attack

7. Conclusion and Future work

The proposed work aimed to investigate the MANET and enhance the MANET routing protocol in order to improve MANET security and communication reliability. In this

context, we first conducted a review of recent developments in the area of MANET. Based on the review we have decided to design an enhanced routing protocol for MANET based on the node capability. That protocol has been named the node capability-based routing (NC-AODV). That is an extension of the traditional AODV routing protocol. The implementation of the NC-AODV routing protocol has been carried out on the basis NS2 network simulator. The comparative study among NC-AODV and AODV demonstrates the superiority of the proposed NC-AODV routing protocol in terms of energy saving, low overhead, higher PDR, and enhanced throughput. However, the protocol works fine but we are interested to improve this protocol for involving security features. Thus we have proposed a Trust-based NC-AODV which is named TNC-AODV. This routing protocol has also verified the normal communication scenarios which demonstrate effective and improved results as compared to NC-AODV. Finally, we have investigated the security aspect of the TNC-AODV routing protocol under the different security attacks. Thus we have considered three MANET attacks namely Black-hole attack, wormhole attack, and DOS flooding attack. Additionally, under the attack conditions, we have verified the performance of AODV, NC-AODV, and TNC-AODV. The performance under attack conditions demonstrates the potential of the NC-AODV and TNC-AODV for dealing with these attacks. However, the NC-AODV has demonstrated the fewer or lower end of performance under attack but with stand-in attack situation, but TNC-AODV has worked fine and provides better security and reliable communication even when the attacks on the network have deployed. The TNC-AODV also works better till 300 nodes reliably and securely.

MANET is an innovative concept and now in these days in a number of real-world networks, we are utilizing the concept of MANET (i.e. IoT and WSN). The network is suffering from different constraints of resources and security. Thus security is an essential perspective of MANET. In addition, the proposed work describes an effort for improving the MANET, but still, we need continuous improvements for adopting new generation applications. Thus the following future extensions are proposed:

1. The MANET need some authentication process to be involved during the joining of the network topology or infrastructure
2. The MANET needs to establish a Machine learning model which will keep an eye on the network using the service provider's server
3. Need to test the MANET security concepts on the new kinds of cyber attacks because after the evolution of 5G the network is more prone to security attacks.

Acknowledgements

We thank our colleagues from Shri Vaishnav Vidyapeeth Vishwavidyala Indore, who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper. This research in funded by any organization.

Author contributions

Mohan Patsariya1: Conceptualization, Methodology, Software, Field study**,** Data curation, Writing-Original draft preparation, Software, Validation, Field Study,

Anand Rajavat 2: Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] S. Tyagi, S. Som, Q. P. Rana, "A Reliability Based Variant of AODV In MANETs: Proposal, Analysis And Comparison", Procedia Computer Science 79 (2016) 903 – 911

[2] H. Yang, "A Study on Improving Secure Routing Performance Using Trust Model in MANET", Hindawi Mobile Information Systems Volume 2020, Article ID 8819587, 17 pages

[3] L. R. Raju, C. R. K. Reddy, "Node activity based trust and reputation estimation approach for secure and QoS routing in MANET", International Journal of Electrical and Computer Engineering, Vol. 9, No. 6, December 2019, pp. 5340~5350

[4] D. A. Kumar, S. Nyamathulla, M. Kirankumar, K. V. Kumar, T. Jayasankar, "A Hybrid Secure Aware Routing Protocol for Authentication in MANET", International Journal of Advanced Science and Technology Vol. 29, No. 03, (2020), pp. 8786 – 8794

[5] V. Tilwari, R. Maheswar, P. Jayarajan, T. V. P. Sundararajan, M. N. Hindia, K. Dimyati, H. Ojukwu, I. S. Amiri, "MCLMR: A Multicriteria Based Multipath Routing in the Mobile Ad Hoc Networks", Wireless Personal Communications, https://doi.org/10.1007/s11277-020-07159-8

[6] B. V. S. Kumar, N. Padmavathy, "A Hybrid Link Reliability Model for Estimating Path Reliability of Mobile Ad Hoc Network", Procedia Computer Science 171 (2020) 2177–2185

[7] B. Safdar, T. Raza, M. Jan, S. Afsar, A. Mateen, Q. Shahzad, M. Azeem, M. Yasir, M. Naveed, "Enhanced-AODV Node Reliability Approach for MANET to Optimize Performance Metrics and Energy Consumption", International Journal of

Advanced Trends in Computer Science and Engineering, 10(2), March - April 2021, 1418 – 1425

[8] M. S. Pathan, N. Zhu, J. He, Z. A. Zardari, M. Q. Memon, M. I. Hussain, "An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs", Future Internet 2018, 10, 16; doi:10.3390/fi10020016

[9] M. G. vaighan, M. A. J. Jamali, "A multipath QoS multicast routing protocol based on link stability and route reliability in mobile ad-hoc networks", J Ambient Intell Human Comput DOI 10.1007/s12652-017-0609-y

[10] M. B. Dsouza, D. H. Manjaiah, "Improving the QoS of Multipath Routing in MANET by Considering Reliable Node and Stable Link", Lecture Notes on Data Engineering and Communications Technologies 55, https://doi.org/10.1007/978-981-15-8677-4_43

[11] D. H. Cho, Y. D. Yeol, C. G. Hwang, "Design of Stochastic Movement Model Considering Sensor Node Reliability and Energy Efficiency", International Journal of Internet, Broadcasting and Communication Vol.12 No.3 156-162 (2020)

[12] D. Sinwar, N. Sharma, S. K. Maakar, S. Kumar, "Analysis and comparison of ant colony optimization algorithm with DSDV, AODV, and AOMDV based on shortest path in MANET", Journal of Information & Optimization Sciences, Vol. 41 (2020), No. 2, pp. 621–632

[13] W. Alnumay, U. Ghosh, P. Chatterjee, "A Trust-Based Predictive Model for Mobile Ad Hoc Network in Internet of Things", Sensors 2019, 19, 1467; doi:10.3390/s19061467

[14] V. S. Ingle, P. Pahadiya, "Trust Based Protected Routing in MANET", Journal of Emerging Technologies and Innovative Research (JETIR), March 2020, Volume 7, Issue 3

[15] M. Ponguwala, DR. S. Rao, "Secure Group based Routing and Flawless Trust Formulation in MANET using Unsupervised Machine Learning Approach for IoT Applications", EAI Endorsed Transactions on Energy Web 06 2019 - 10 2019 | Volume 6 | Issue 24 | e4

[16] Dr. S. Ramesh, "Protected Reliable Routing For MANET Using Bees Algorithm", © 2018 Swansea Printing Technology Ltd, 2241 Taga Journal Vol. 14.

[17] S. Naveena, C. Senthilkumar, T. Manikandan, "Analysis and Countermeasures of Black-Hole Attack in MANET by Employing Trust-Based Routing", 6th International Conference on Advanced Computing & Communication Systems, 978-1-7281-5197-7/20/$31.00 ©2020 IEEE

[18] R. Tourani, G. Torres, S. Misra, "PERSIA: a PuzzlE-based InteReSt Flooding Attack Countermeasure", 7th ACM Conference on Information-Centric Networking, 2020, Virtual Event, Canada. ACM, New York, NY, USA, 12 pages

[19] D. Chouhan, Asst. Prof. A. Pal, "Detection and Mitigation of Mitigate Denial of Service (Dos) Attacks Using Trust-Based Mechanism", International Journal of Scientific Research & Engineering Trends, Volume 7, Issue 4, July-Aug-2021

[20] K. G. Reddy, P. S. Thilagam, "Naïve Bayes Classifier to Mitigate the DDoS Attacks Severity in Ad-Hoc Networks", International Journal of Communication Networks and Information Security, Vol. 12, No. 2, August 2020

[21] N. Veeraiah, O. I. Khalaf, C. V. P. R. Prasad, Y. Alotaibi, A. Alsufyani, S. A. Alghamdi, N. Alsufyani, "Trust Aware Secure Energy Efficient Hybrid Protocol for MANET", IEEE Access, VOLUME 9, 2021

[22] R. Pandey, Prof. P. Tripathi, "Detection and Prevention of Wormhole Attack using the Trust-Based Routing System", International Journal of Scientific Research & Engineering Trends, Volume 7, Issue 4, July-Aug-2021

[23] F. H. Tseng, H. P. Chiang, H. C. Chao, "Black Hole along with Other Attacks in MANETs: A Survey", J Inf Process Syst, Vol.14, No.1, pp.56~78, February 2018

[24] M. Shukla, B. K. Joshi, U. Singh, "Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET", Wireless Personal Communications (2021) 121:503–526

[25] M. Patsariya and A. Rajavat, "Network Path Capability Identification and Performance analysis of Mobile Ad hoc Network," 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, 2020, pp. 82-87, doi: 10.1109/CSNT48778.2020.9115772.

[26] Patsariya M, Rajavat A. A survey on node capability based trusted routing in MANET: issues & challenges. *IJCSNT*. 2019; 8(1).

[27] M. Patsariya and A. Rajavat, "Hybrid Routing Approach with Energy Aware for Minimize Routing Overhead in MANET," 2013 International Conference on Communication Systems and Network Technologies, Gwalior, India, 2013, pp. 236-242, doi:

10.1109/CSNT.2013.57.

[28] M. Patsariya and A. Rajavat, "Hybrid Routing Approach and WIMAX Network for Minimization Routing Overhead and Increasing Radio Range in MANET," 2012 Fourth International Conference on Computational Intelligence and Communication Networks, Mathura, India, 2012, pp. 127-134, doi: 10.1109/CICN.2012.127.

[29] Singh, U., Shukla, M., Jain, A.K., Patsariya, M., Itare, R., Yadav, S. (2020). Trust Based Model for Mobile Ad-Hoc Network in Internet of Things. In: Smys, S., Bestak, R., Rocha, Á. (eds) Inventive Computation Technologies. ICICIT 2019. Lecture Notes in Networks and Systems, vol 98. Springer, Cham. https://doi.org/10.1007/978-3-030-33846-6_90