International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

A Trust and Node Capability Model for Reliable and Secure MANET Communication

Mohan Patsariya
Department of Computer Science & Engineering,
Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, 453331, India
E-mail: mohan.patsariya@gmail.com

Anand Rajavat
Department of Computer Science & Engineering,
Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, 453331, India
E-mail: anandrajavat@yahoo.co.in

*Abstract***:** The Mobile Ad-hoc Network (MANET) is a rapidly deployable network. That is valuable for industrial and domestic applications due to flexible, mobile, and wireless communication. But the network is constrained with resources and security. In this paper, we are presenting a node capability based trusted routing named TNC-AODV for MANET. It is a hybrid approach for maintaining route reliability and security. The model is composed of the property of node capability and Trust. The Node capability is defined by the quality of service parameters like remaining energy, available bandwidth, buffer length, and mobility pattern. The aim is to ensure the discovery of reliable routes. Additionally, the trust is implemented by using a local and global trust for securing the network. The TNC-AODV is implemented through modification of AODV routing. That routing technique has been tested on three security threats namely Black-hole, wormhole, and DOS flooding attack. The simulation has been carried out using the NS2 simulator. The experimental results demonstrate that TNC-AODV provides security against attacks. Additionally, improve the packet delivery ratio, and throughput. Finally, the possible and feasible future extension of the work has also been proposed.

Index Terms: MANET, Security, Communication Reliability, Node Capability, Trust Management, Secures Routing.

I. INTRODUCTION

The mobile ad-hoc network (MANET) is ad-hoc in nature, which means built with the dynamic network topology created by mobile nodes [1]. There is not any centralized control available thus the network activities are handled by network nodes using routing protocols [2]. The nodes are having limited communication range thus communication is performed by using the intermediate nodes. In order to establish communication, the source router has initiated the route discovery, when the destination router is informed, then the temporary route has been established [3]. The frequent route discovery and establishment consumes the network resources additionally vulnerable to different security threats [4]. Thus we need some techniques for improving communication reliability and security. Because any malicious node can connect with the network and can perform abnormally activates which degrade the network performance [5].

In this paper, we are addressing the issue of reliable and secure route formation for MANET. Therefore, first, we need to understand the issue of security and reliability. In this context, a review of existing security and reliability improvement techniques in MANET has been carried out, and then by utilizing the available concepts we have proposed a new routing algorithm. The proposed algorithm is intended to select efficient and secure routes. Further, the simulation has been carried out based on NS2, and the performance of the proposed routing technique is explained. Finally, the conclusion of the efforts is made and future extension has been provided.

II. RELATED STUDY

This section provides the study of recent studies and enhancements in the MANET routing technology. Thus more than 30 research articles have been collected among 24 which are more relevant to the proposed work has been selected. During the study, we have categorized the entire work for the area of application, the method used, and the consequences of the techniques. According to findings, the techniques based on trust and route reliability can better manage the network quality of service in terms of performance as well as security. The summary of the studied literature has been defined in table 1.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Table 1 Literature Survey

Ref.	Publicat. & year	Area	Method	Results
[6]	Procedia Computer Science 2016	Examined AODV routing protocol	Positive and negative characteristics of AODV for QoS. Routes are constrained with E2E Delay and Bandwidth for QoS.	Reliability aware variant of AODV. Enhance the reliability of intermediate nodes.
[7]	Hindawi Mobile Information Systems, 2020	Method for trust evaluation using cluster and secure key exchange	Used a hierarchical structure for reliability enhancement. Reliability demonstrates quality of packets and packet delivery by the trust management node. Data integrity is improved.	Anomaly nodes are identified. In the presence of malicious nodes, the technique can maintain performance.
[8]	Intern. Jour. of Elec. and Comp. Engg, 2019	Securing and QoS routing using NA-TRE	Tracks the changes of packet drop or forwards to get status of the node. The status is described as Normal State (NS), Resource Limitation State (RS), and Malicious State (MS).	Compared with AODV, FACE, and TMS protocols. Shows enhancement on throughput and reduce in overhead and E2E delay.
[9]	IJAST, 2020	HSARP to balance security and power	Multicast routes discovery and power distribution is used. Secret-sharing is used based on trust.	Enhance energy efficiency
[10]	Wireless Personal Communications,	MCLMR	Select intermediate nodes for route. Consider: nodes mobility, contention window, and link quality	Technique compute weights based on mobility, window size, and link quality, and Expected Number of Transmissions metric is used
[11]	Procedia Computer Science, 2020	Free space two ray ground models for connectivity	Helps in determining network performance. The reliability of homogeneous MANET reduces	Though less reliability values, the network shows reliability
[12]	IJATCSE, 2021	energy-efficient model using AODV	EAODV routing performs better than OLSR. Modified AODV to increase the throughput, E2E delays, packet distribution.	Compare AODV, DSDV, OLSR, and Enhanced AODV. DSDV provides high throughput, lower latency, and high PDR.
[13]	Future Internet, 2018	Trust-based secure QOS routing	Mitigating nodes which are misbehaving in packets forwarding and ensures reliable communication. Select best node based on packet forwarding and capability in terms of channel quality, energy, link quality, etc.	Demonstrate using packet-dropping attack. Trust can enhance security and QoS.
[14]	J Ambient Intell Human Comput	Describe a SR-MQMR	First uses signal strength to choose the nodes. Then, route expiration time and number of hops are used to select a route.	SR-MQMR used less time, decreased overhead, decreased consumed bandwidth, and increase lifetime.
[15]	Lect. Notes on Data Engg and Comm. Techn.	REL-AOMDV		With increase in mobility, REL-AOMDV shows a lower routing overhead and delay.
[16]	International. Journal of Internet, Broadc. and Comm., 2020	Design probabilistic mobile models for MANET.	Dividing moving nodes and distance into two categories. Ensuring that the width and variation rate was stable.	Model of movement by simulation and compared with random movement model. Showing energy efficiency and stability.
[17]	Journal of Information & Optimization Sciences, 2020	Compares AODV, AOMDV, DSDV, and ACOP using Random Waypoint Model	Purpose of using mobility model to generate different scenarios.	The performance of the ACOP is found better than others.
[18]	Sensors, 2019	Quantitative trust model	Combines direct and indirect trust opinions. Beta probabilistic distribution is used.	Theory of ARMA/GARCH used to combine trust evidence and resultant trust.
[	IEEE Access,	Address energy	Trust-based secure energy-efficient	The fuzzy clustering is put

				multipath Routing
[19]	JETIR, 2020	Composite trust metric based on social trust and QoS trust	Extended AODV, and enhance trust model with packet-forwarding misbehaviors.	Provides improvement in packet delivery ratio, routing overhead, and energy consumption.
[20]	EAI Endorsed Transactions on Energy Web, 2019	A security mechanism to protect the MANET-IoT	Cluster-based technique with recommendations by security monitors using unsupervised algorithm. Clustering is done using Secure Certificate-based Group Formation and K-means is used for trust.	For secure route selection, a hybrid algorithm based on the Genetic and FireFly Algorithm (GA-FFA).
[21]	Swansea Printing Technology Ltd, Taga Journal 2018	Protected Reliable Routing (PRR) for security	Two way secured encrypted that cross-validate for multicast communication and MD5 and HMAC is used for unicast communication. Bees algorithm.	Avoid delay
[22]	ICACCS, IEEE 2020	Black-hole attack	Trust-based routing. secure routing into two stages	Identify and preserve data transfer mechanism and predict a safe path
[23]	ACM Conf. on Info.-Cent. Net., 2020	PERSIA, distributed request flooding prevention, and mitigation system	Eliminates the possibility of attacks. Dynamically deploys an in-network mitigation strategy	Demonstrate resiliency and effectiveness
[24]	IJSRET, 2021	Detect and eliminate DoS and DDoS attacks	entropy-based technique	
[25]	IJCNIS, 2020	DDoS attack severity mitigation	A node authentication and naïve Bayes classifier to detect and isolate attack.	Naïve Bayes-based classification outperforms and secures the traffic.
[26]	IEEE Access, 2021	Address energy efficiency and security	Trust-based secure energy-efficient navigation, Selects the jumps in advancing the routing	The fuzzy clustering is put on, and the cluster heads (CHs) are picked predicated maximum worth of trust.
[27]	IJSRET, 2021	Collection of wormhole nodes is called a communitarian attack	Deal with attacks using Trust esteem	Trusted AODV protocol is improvement on standard AODV.
[28]	J Inf Process Syst, 2018	survey of the black hole in MANETs	Include survey of published article in past 5 years. Considered non-cooperative and collaborative attacks. Wormhole and flooding attacks also studied	Conceive the open issues and future trends of black hole detection and prevention.
[29]	Wireless Personal Comm., 2021	black hole and wormhole attack	two types of protocol AODV and the scalable-dynamic elliptic curve cryptography	SWBAODV were good compared with the BAODV and WAODV

In addition, some essential keywords are also identified. Table 2 contains the list of frequently used keywords in the studied literature.

Table 2 Abbreviations

S. No.	Abbreviation	Full Form
1	AODV	Ad hoc On-Demand Distance Vector
2	QoS	Quality of Service
3	E2E	End-to-End
4	NA-TRE	Node Activity-based Trust and Reputation estimation
5	HSARP	Hybrid Secure Aware Routing Protocol
6	MCLMR	Mobility, Contention window, and Link quality sensitive
7	SR-MQMR	stable and reliable multi-path QoS multicast routing protocol
8	REL-AOMDV	Reliable energy and link AOMDV

III. Proposed Routing Technique

The aim is to introduce an algorithm for MANET for secure and reliable communication. The algorithm incorporates node capability-based route formation and includes trust management for mitigating security issue of the network. The node capability is defined by remain energy E, remain buffer storage B, mobility of node M and available bandwidth AB. The energy resourceful nodes are able to provide stability in

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

network service. Let the node has an initial energy level E_I and in a time period Δt the node consume e amount of energy then the total remain energy is given by:

$$E = E_I - e \dots\dots\dots\dots\dots (1)$$

$$B = B_L - B_c \dots\dots\dots\dots\dots\dots (2)$$

Next, we considered the mobility of the node, because a highly moving node is not suitable for reliable path creation. But the mobility in a small area is not much affecting the performance. Therefore we are computing the displacement of a node. Let a node has initial coordinates (x_1, y_1) and after a sample time Δt the new position of node is (x_2, y_2). Thus the total displacement M of node is:

$$M = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \dots\dots\dots\dots\dots (3)$$

The bandwidth is also an essential parameter for effective route selection. If the link between two nodes has low bandwidth then the transmission speed becomes slowed down thus we need to utilize those links which have a sufficient amount of bandwidth available. Thus, if the link between two nodes has AB_I bandwidth and currently transmitting the data with ab speed then the total available bandwidth is:

$$AB = AB_I - ab \dots\dots\dots\dots\dots\dots\dots (4)$$

The node capability is providing grantee the with quality of service. The considered quality of service parameters is used for selecting the capable nodes for the formation of routes. But the question is how we are going to discover and establish a capable route. In this context, we utilize the following steps to discover and established a route:

3.1. Route Discovery

In ad-hoc networks, route discovery is an essential step of routing. Using this process the router discovers the shortest path between source and destination. Here the aim is not only to find the shortest path, it is also required the route is efficient and reliable. Therefore, in this work, we have considered the AODV routing protocol for implementing the required process of efficient and reliable route selection. In the route discovery process, the source node initiates with flooding Route Request (RREQ) packets. When the destination node received a route request in response, the Route Response (RREP) message is flooded, on receiving the RREP message to source node a reverse route has been created. However, in normal AODV routing when the reverse route is created the AODV starts the data transmission. Therefore, before initiating the transmission we need to perform the route quality check.

3.2. Evaluation of Route

The route quality depends on the intermediate node's quality. In this experiment, we utilize the node capability as the node quality parameter. The node capability has involve the fractions of remaining energy, buffer length, mobility, and available bandwidth. But these values are calculated on different scales therefore we normalize these values using the min-max method using the following equation:

$$NormValue = \frac{val - min}{max - min} \dots\dots\dots\dots (5)$$

We define the equation (1) in such manner,

$$nE = E * 0.01 \dots\dots\dots\dots\dots (6)$$

Because, the maximum energy level is considered as 100 and minimum energy is 0. Next, we recreate the equation (2) as,

$$nB = B * 0.01 \dots\dots\dots\dots\dots\dots (7)$$

Because, the maximum buffer length is considered as 100 and minimum energy is 0. Next parameter is mobility, here we have consider the maximum mobility 5 meters and minimum 0 meter. Therefore, the equation (3) can be written as:

$$nM = M * 0.2 \dots\dots\dots\dots\dots\dots (8)$$

Because we assume that the mobility of more the 5 meters in a sample time can majorly affect the performance. As we decrease the mobility maximum value. The stability of the network path will be increased. Finally, we considered the available bandwidth. Here we consider the 1MB as the initially available bandwidth. Therefore we have not changed the scale of AB. Finally, we compute node capability as:

$$NC = \frac{nE + nB + nM + AB}{4} \dots\dots\dots\dots\dots (9)$$

The NC is the indicator of node quality and reliability, the value of NC is varying between 0-1.

3.3. Decision of Route

After measuring the node capability NC, we need a threshold value to decide whether a route is reliable or not. In this context, we have calculated a threshold separately, for this purpose we have prepared a network and performed the communication among three different sources and destinations. Additionally, we calculated the NC of the intermediate nodes. Using the NC values of the N intermediate node the value of route reliability R is measured using the following formula:

$$R = \frac{1}{N}\sum_{i=1}^{N} NC_i \dots\dots\dots\dots\dots\dots (10)$$

Here we use three scenarios of communication for measuring the threshold thus the threshold value is estimated as:

$$T = \frac{R_1 + R_2 + R_3}{3} \dots\dots\dots\dots\dots\dots (11)$$

This threshold will be used for deciding the route reliability. Here it is assumed that if the route's reliability *R* is higher than the threshold's 75%, then we have marked the route as a reliable route. The following function will be used for deciding the route is suitable or not.

$$f(R) = \begin{cases} if\ R > T * 0.75\ Then\ Mark = 1 \\ Otherwise\ Mark = 0 \end{cases} \dots\dots\dots (12)$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

According to equation (12) if the f(R) is 1 then we reliably transmit the data otherwise not. If f(R) results in 0 then we discard the current route and start the evaluation of the next reverse route. This process is named here Node Capability Based AODV (NC-AODV). The aim is not only to provide reliable communication we need security also. Thus we extend the NC-AODV for security by using a trust management scheme. The trust minimizes the risk of compromising the network against security threats. The proposed trust scheme is composed of two fractions i.e. local and global trust. The global trust is denoted as G, which demonstrates the historical social trust. That is calculated by three neighbors' opinion O. If the neighbor nodes respond the node is interacted before then the algorithm assigns it 1, otherwise 0. Using these opinions, we are computing the global trust as:

$$G = \frac{1}{N}\sum_{i=1}^{n} O_i \dots\dots\dots\dots\dots\dots\dots (13)$$

Where N=3, that can be regulated according to security level requirements. Next component is Local trust, which is defined by the route. In order to compute the local trust the following function will be used:

$$L = \frac{rE + F + P + AB}{4} \dots\dots\dots\dots\dots (14)$$

Where, L = Local Trust, rE = Energy Remain: if % of energy remain > 33%, then E =1, F = amount of RREQ flooding is less then T_{RREQ}, then F =1, P = Packet delivery ratio in % is > 60%, then P = 1, AB = Available bandwidth in % is > 33% then AB = 1. Finally, based on individual node's local trust we calculate the local trust for entire route using following equation:

$$L_R = \frac{1}{N}\sum_{i=1}^{N} L_i \dots\dots\dots\dots\dots\dots (15)$$

Where, N = number of nodes in route, L_i = Trust of ith node, L_R = Local Trust for the entire route

Finally we are measuring the combined trust of route using:

$$TR = \frac{G + L_R}{2} \dots\dots\dots\dots\dots (16)$$

According to the combined trust value if TR higher than 70% then we consider the route is safe otherwise we discard the route and again route discovery performed. The combined process of managing the reliability and security in a common protocol is named here as trust-based NC-AODV (TNC-AODV).

V. Results Analysis

The aim is to achieve a reliable and secure routing for MANET. Therefore we evaluate the performance of the TNC-AODV under the security threat and also offer a comparative study with NC-AODV and classical AODV. The considered attack models are namely Black-hole attack, wormhole attack, and DOS flooding attack.

4.1. Attack Models

Black-hole Attack: In this attack, the attacker has trying to eliminate the packets from the network. The attacker is start working when the source router initiates the route discovery. During this source node floods RREQ for getting an efficient route and when the malicious node found the request message then the malicious node keeps the RREQ message and replays it with a false Route reply message (RREP). The source node gets the reply and then starts communication by using the attacker node. The attacker node drops all the packets to degrade the performance.

Wormhole Attack: the wormhole attack is also a performance-degrading attack in MANET. In this attack, at least two or more attackers are required to mislead the communication. In this attack, two or more attackers are creating a high-speed link this link is called a wormhole link or wormhole tunnel. Due to the higher speed of this link, the network functions become imbalanced, additionally, network nodes start communicating with this link and congestion has formed. Due to this congestion, most of the packets are dropped and network performance has been degraded.

DoS Flooding Attack: the main aim of DOS flooding attack deployment is to prevent a target or specific node from getting network services. Therefore the attacker node continuously floods the route request packets to the victim node. The victim node has started working on these packets and soon stops working. The victim node is not able to send or receive any packet.

4.2. Performance evaluation

In order to evaluate and compare the performance of the AODV, NC-AODV, and TNC-AODV we have deployed attacks in the network. Additionally, the simulation with different network sizes has been carried out. After simulation, the mean performance of the networks is recorded and described in this section.

First, we have implemented DDOS attack, Black-hole attack, and wormhole attack to all three configured networks based on the AODV, NC-AODV, and TNC-AODV routing protocol. Additionally, the mean performance in the described scenario has been measured and reported in figure 1 and figure 2. The performance in terms of End to End (E2E) Delay which is shown in figure 1(A) shows the E2E delay of implemented protocols under attacks. The obtained performance of NC-AODV and TNC-AODV demonstrate similar behavior. On the other hand, the AODV routing protocol shows minimum delay due to no packets being exchanged during the attack situation. However, the network based on NC-AODV has been impacted due to attacks but is able to provide the services. But the TNC-AODV routing has demonstrated the avoidance ability against the attacks.

The energy consumption of the implemented routing techniques is given in figure 1(B). The obtained results demonstrate the higher energy consumption of the AODV routing protocol, the NC-AODV routing protocol, and the lowest energy consumption found with the TNC-AODV. Therefore we can say the attacks can increase the energy

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

consumption of the routing protocols but the avoidance techniques implemented with TNC-AODV reduce the effect of attacks thus the TNC-AODV is a reliable and secure routing as compared to NC-AODV and simple AODV. The next evaluation parameter of the routing techniques is the routing overhead, which is reported in figure 1(C). The overhead of AODV is higher than both the other routing protocols. The routing overhead demonstrates the additional packets injected into the network during the communication. the routing overhead of the protocols is increased due to the attack conditions, but the TNC-AODV routing protocol shows minimum overhead as compared to the NC-AODV and simple AODV routing protocol.

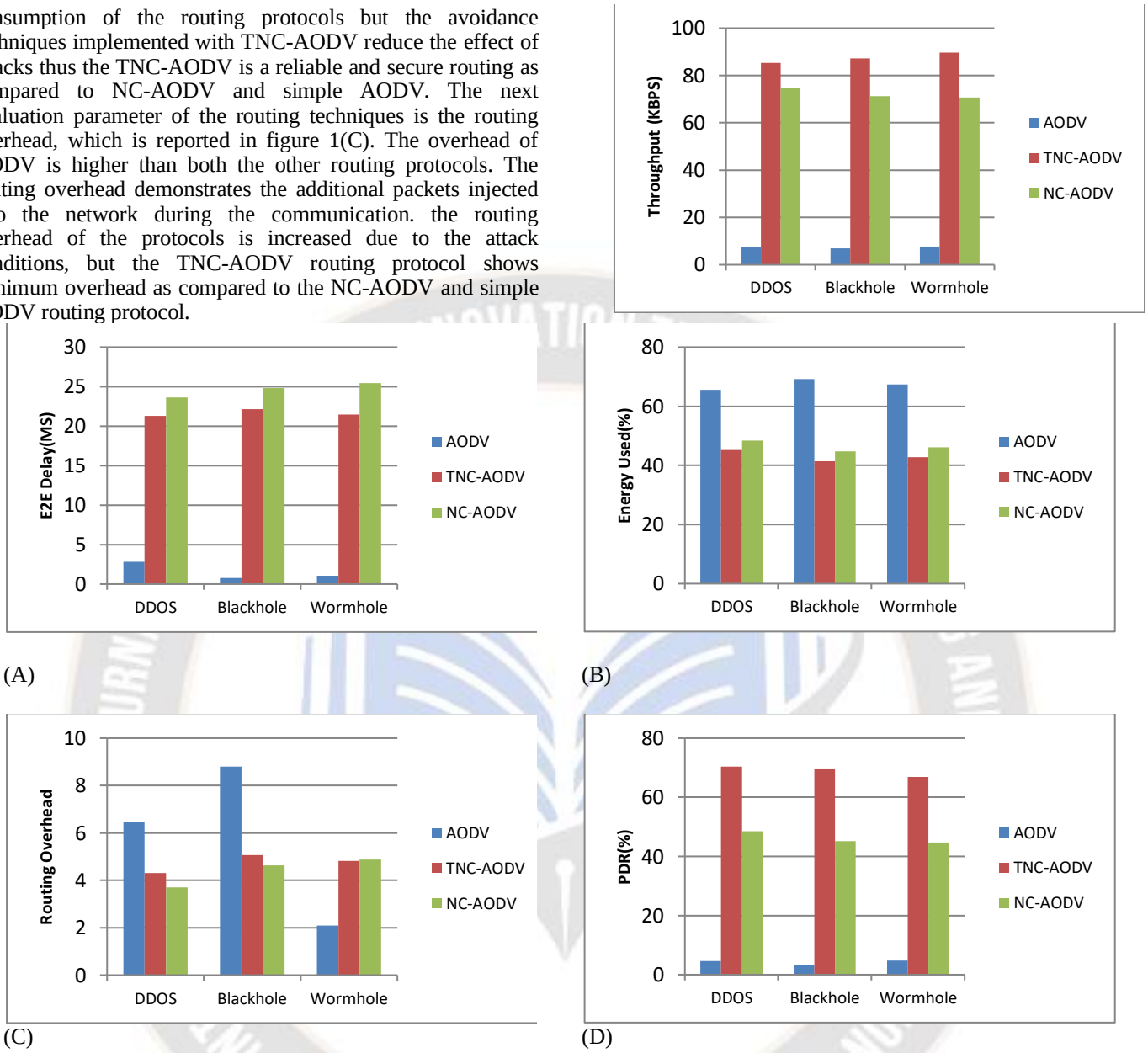

Fig. 1. Shows The Comparative Performance Of Three Routing Algorithms In Terms Of (A) E2E delay (B) Energy consumption (C) Routing Overhead and (D) Packet Delivery Ratio

The packet delivery ratio of the implemented routing algorithms is given in figure 1(D). According to the implemented attack properties, these attacks are interrupting communication thus it significantly reduces the network performance in terms of PDR. According to the obtained performance in this experiment, we have found that the AODV demonstrates the minimum PDR. Additionally, NC-AODV and TNC-AODV routing protocols show improved performance as compared to traditional AODV routing. Thus both the protocols are able to reduce the impact of the attacks in all the scenarios of the experiment.

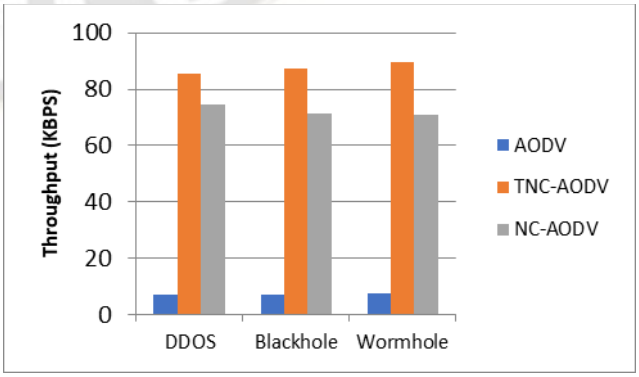

Fig. 2. Throughput of Three Routing Algorithm

The next parameter of evaluation is throughput which is demonstrated in figure 2. Here due to the influence of attacks, the throughput of AODV routing is very fewer. On the other hand, the NC-AODV and TNC-AODV routing can show strength against the attacks. Therefore we can see in figure 3 the throughput of TNC-AODV and NC-AODV is higher enough than the AODV routing protocol. Thus these two algorithms are reliable and secure as compared to AODV.

5. Conclusion and Future Work

The proposed work aimed to enhance the MANET routing in order to improve security and reliability. In this context, we first conducted a review of recent developments in MANET. Based on the review we have decided to design an enhanced routing protocol based on the node capability and trust. Thus we have proposed a Trust-based NC-AODV (TNC-AODV). This routing has been verified under the different security attacks namely Blackhole attack, wormhole attack, and DOS flooding attack. The performance under attack conditions demonstrates the potential of the NC-AODV and TNC-AODV. The TNC-AODV has provided better security and reliable communication. However the proposed work describes the improved technique of the MANET, but for increasing demand and security threats in different applications, we need continuous efforts of improvements. Thus the following extensions are proposed:

1. The MANET needs to establish a Machine learning model which will keep an eye on the network
2. Need a dynamic scalability and authentication technique for adopting new nodes in the network

Compliance with Ethical Standards:

(a) Conflicts of interest: Authors A declares that he has no conflict of interest. Author B declares that he has no conflict of interest.

(b) Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

(c) Funding: This study is not funded and none of the author has been received any grant for this article.

REFERENCES

[1] M. Z. Hussainf, M. Z. Hasan, Z. Ullah, “Mobile Ad-Hoc Networking (MANET)”, UW Journal of Computer Science, Vol. 03, 09-18

[2] V. Rajeshkumar, P.Sivakumar, “Comparative Study of AODV, DSDV and DSR Routing Protocols in MANET Using Network Simulator-2”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 12, December 2013

[3] R. Raju L., 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] F. A. Fattah, F. AlTamimi, K. A. Farhan, F. H. Al-Tarawneh, “Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs”, IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology, 978-1-5386-7942-5/19/$31.00 ©2019 IEEE

[5] G. Singh, Dr. O. P. Dubey, G. kumar, “A Solution to Selective Forward Attack in Wireless Sensor Network”, International Journal of Students’ Research in Technology & Management, Vol 6, No 4, 2018, pp 01-06

[6] 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

[7] 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

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] 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

[16] 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)

[17] 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

[18] 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

[19] V. S. Ingle, P. Pahadiya, “Trust Based Protected Routing in MANET”, Journal of Emerging Technologies and Innovative Research, March 2020, Volume 7, Issue 3

[20] 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, 2019, Volume 6, Issue 24, e4

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

[22] 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

[23] 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

[24] 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

[25] 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

[26] 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

[27] 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
[28] 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
[29] 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