Security for Multipath Routing Protocol using Trust based AOMDV In MANETs

***K. Vinayakan,**
PG & Research Department of Computer Science, Khadir Mohideen College, Adirampattinam (Affiliated to Bharathidasan University, Tiruchirappalli)

M. V. Srinath,
Department of MCA, Sengamala Thayaar Educational Trust Women's College, Mannargudi (Affiliated to Bharathidasan University, Tiruchirappalli)

A. Adhiselvam,
Department of Information Technology, Dr. N.G.P. Arts and Science College, Coimbatore

Abstract

Mobile Ad Hoc Networks (MANETs) provide a vibrant atmosphere wherein data may be substituted deprived of the necessity of a human authority or centralized server, as long as nodes work together for routing. As long as security throughout the multipath routing protocol and data transfer over many routes in a MANET is a difficult problem, this work offers a message security technique that joins multipath (Ad hoc on Demand Multipath Distance Vector) AOMDV routing established on trust with soft encryption in MANETs, resulting in Trust based Ad hoc on Demand Multipath Distance Vector (T-AOMDV) protocol. By utilizing signatures that are digitized for route discovery in this system, Route Request (RREQ) packets have been signed for securing multipath routing and data transmission. The destination validates entire signatures and stores the route list utilizing session key of source node while obtaining first RREQ packets from the node. Route Reply (RREP) has been sent over same route to its source node. Its route will be allowed if the signature is confirmed. The message parts are encrypted at source node by means of hash function and a session keys. Secure routing may be done established on the trust value of nodes. An algorithm is utilized to select the most secure routing path possible. After that, messages are split into soft encrypted and XOR operations are done on them. The original message is decrypted and recovered by destination node. The system is considerably more secure than standard multipath routing algorithms, according to simulation findings using ns2. When compared to Trust based Dynamic Source Routing (T-DSR) system, the suggested T-AOMDV configuration provides a quickest route selection time. In all situations, both T-AOMDV and T-DSR systems contain zero trust compromise.

Keywords: MANET, Multipath, Routing Protocol, T- AOMDV, RREQ, RREP

1. Introduction

MANETs comprises assembly of mobile nodes that are wireless and may enthusiastically interchange data deprived of the need for a cable backbone network or a fixed base station. MANET nodes are characterized by their memory resources, inadequate power, processing and also their great mobility. Numerous routing protocols like Ad-hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) might be utilized in MANET. Nevertheless, owing to instability of wireless medium and dynamic topology caused by node movement or failure, communication failures are common and route re-establishments take a long time.

Multipath routing allows nodes to interconnect across several pathways inside the transmission range, allowing for operative communication between transmitters which could be contained inside the wireless range of one another [1].As multiple fragmented paths may exist between nodes, multipath routing may be utilized for improving the secrecy of exchanged messages amid destination and source nodes by means of statistics. Transferring confidential data over a single path makes it easier for attackers to obtain entire data, but delivering it in bits across several disconnected channels enhances confidentiality robustness, since obtaining all portions of a message that has been split and transmitted over multiple paths amongst the destination and source is very challenging. Since using many routes can reduce the impact of probable node and link failures, a multipath routing protocol is a viable approach for overcoming difficulties of connection improbability and recurrent topological alterations.

Multipath ad hoc routing protocols outperform single-path routing methods due to resilience, enhanced dependability, reduced end-to-end time, load balancing and security. Node failures, crowded links or nodes, link failures, transmission errors and route breakages are all common routing problems in MANETs. Owing to multipath routing, there are more collisions across associated paths that lower network performance (i.e. packet delivery ratio). The nodes in a MANET system might potentially be selfish and malevolent. Selfish behaviour may cause packets to be dropped, whereas malevolent activity may result in passive or aggressive attacks and reducing the data transfer's dependability.

1.1 Secure multipath routing in MANET

The existence of rogue nodes might raise severe issues about message security. Message availability, message secrecy and node authentication are some of these problems. Because of these cooperative routing difficulties, achieving comprehensive message security in MANETs remains a difficulty. Integrity, confidentiality, authentication and non-reputation are all features of security systems. The identification of a passive attack is difficult in this case since the network's functionality remains unaffected. Using a strong encryption method to encrypt data being transferred is one of the answers to such problem. Likewise, active attack aims to modify and delete data that is exchanged across network causing network's regular operation to be disrupted. Internal or external active attacks are also possible. Nodes that aren't linked to network conduct external attacks, whereas an inside attack that has been launched by network nodes that have been hacked. When the nodes carry out active attacks such as modification, fabrication, impersonation and duplication, they are referred to as active attacks. Any layer of the network protocol stack can be attacked passively or actively. Grey hole attack, resource consumption attack, rushing attack, wormhole attack including black hole attack are the currently active attack parameters [2].This work introduces T-AOMDV, a safe message security system for MANETs that combines multipath AOMDV routing and are trust-based by means of soft-encryption process to secure message transmission.
The strategy comprises of three phases in total: (1) Message encryption - A message is divided into three sections at source node and using XOR operations it is encrypted subsequently. (2) Message routing -Using a new AOMDV protocol with nodes that are disjoint, the message portions are routed independently over various trust-based multiple

routes and (3) Message decryption - For reclaiming original message, the message portion is decrypted by destination node [3]. This work offers a message security technique which joins multipath AOMDV routing established on trust with soft encryption in MANETs, resulting in T-AOMDV system. Standard multipath routing systems for MANETs including a newly recommended message security method are substantially less secure than the system, demonstrated by simulation results using ns2. In performance benchmarks, trust breach and route selection time are utilized.

The Literature survey discussed in section 2 which is based on the Securing multipath routing method, Section 3 defines the proposed technique for protecting the multipath AOMDV routing protocol, Section 4 provides the outcomes and comments based on evaluation results and this section 5 discusses concludes.

2. Literature Review

Sahu et al. investigated the depiction of a multipath routing approach that iszone-based, termed as Zone-Based Leader Election Energy Constrained AOMDV Routing Protocol (ZBLE) for MANETs. [4]. The main goal of MANETs is confirming the quality of network by making communication of system effective and efficient. When compared to standard route protocols like AOMDV and AODV, they are outperformed by ZBLE protocol. To improve the MANET's overall performance, Sirajuddin et al. [5] propose a Trust-Based Secure Multipath Routing Protocol(TBSMR). The proposed protocol's major strength is that it considers various variables to improve the MANET's QoS, such as malicious node identification, packet loss reduction, congestion control and secure data transfer. A simulation in NS2 is used to evaluate the proposed protocol's performance. The suggested routing protocol outperforms the existing methods, according to simulation results.

Sarbhukan and Ragha [6] designed a MANET infrastructure that allows any flexible node to simply take part in data transmission and connect the network. For dealing with congestion, Jhajj et al. [7] proposed the EMAODV protocol. The Time-To-Live (TTL) value is used in this protocol to prevent RREQ packet flooding. This TTL value is utilized to determine which nodes are active for packet forwarding. For packet forwarding, only these active nodes are needed. Other node that doesn’t react to RREQ packets are contemplated as silent nodes and do not participate in routing unlike active nodes.

The Levenberg-Marquardt Neural Network (LEACH-LMNN) protocol is divided into two sections, according to Mittal et al [8] and they are: LMNN method is used to choose the cluster head node and the second section involves in using multiple route discovery techniques to determine the minimal path to base-station node from cluster-head node that is Dijkstra, Bellman-Ford and breadth-first search. The simulation findings displaya LEACH-LMNN protocol, which uses Dijkstra shortest path algorithm and leaves behind other alternate route discovery approaches.

For MANET route optimization, Sarkar et al. [9] introduced a newly designed Ant-AODV protocol. Established on ant colony optimization idea, identification of optimum routes is done in this protocol. Routing is accomplished using this method by determining the pheromone values of all possible routes. Packets will be sent from source to destination via

the path with greatest pheromone levels. To tackle the optimization challenge in real-time network context, Robinson et al. [10] offers a new link-disjoint multipath routing technique. Hence in MANETs, the suggested approach is utilized to select the shortest path among numerous pathways. The suggested approach operates effectively in a dynamic network context, according to simulation findings.

Angurala et al. [11] compare AOMDV and load balanced AOMDV with various factors such as routing overhead and delay. NS2 Simulator is used to implement the suggested task. Furthermore, the findings show that this new technique may reduce routing cost and latency without increasing network overhead. When compared to normal AOMDV protocol, energy usage is likewise quite low in this situation. In AOMDV method, fitness function has been employed for determining an optimal path as stated by Jain et al [12].The function in this study takes into account not just residual energy; it includes the nodes transmission power in network as well.

The T-AOMDV system proposed by Huang et al.[13]is a MANETs message security system that uses trust-based multipath AOMDV routing and soft encryption. Furthermore, a method for computing a quantitative estimate of the risk involved with a topic is offered by the fuzzy multilevel security. Through packet monitoring and node activity, the trust mechanism supports the notion of recognizing hostile nodes. If a trust value is insufficient, the selected path will not be secure for transmitting all data and the procedure will be repeated. To securely transfer messages on MANETs, Woungang et al. [14] present an improved trust-based multipath DSR protocol. A trust management mechanism, soft encryption and multipath DSR routing make up this technique. The interactions module history keeps the records of interactions amid nodes in an appropriate data format. Each contact between nodes is preceded by a calculation of trust.

Zeyad and Riyaz's [15] research on MANETs is primarily focused on the characteristics of multipath routing protocols. Two multipath routing protocols is examined and an evaluation study using simulation NS2 is conducted amongst DSR and AODV in order to offer an improved way to reaching the target while maintaining QoS. The simulation demonstrates that variations in a protocol resulted in significant variances in its performance. Bhagyalakshmi et al. [16] introduced the Q-AODV protocol, which uses queue vacancy parameter to identify a non-congested route. The queue vacancy factor is utilized for reducing intermediate nodes quantity in route exposure state, which reduces the transmission of control packets.

According to Hussain and Khan [17], the TBSMR protocol is AODV protocol’s modified version. TBSMR protocol resolves the AODV protocol's shortcomings. Malevolent nodes are identified in TBSMR protocol during all level of communication. Furthermore, the packet loss reduction technique is utilized to ensure that packets are delivered reliably. During the first route disclosure phase, source node broadcasts a bogus RREQ in this protocol. This bogus RREQ packet has a fictitious destination sequence and destination address numeric figure. To such false RREQ message, merely a malicious node replies through a RREP packet appealing to have the best route to the target [18].

Rahul et al.[19] explores a number of multipath routing techniques for MANET. Routing protocols are also divided into several categories to provide load balancing, dependable

communication and improved MANET service quality. Chen et al. [20] provide a Topological change Adaptive model Ad hoc On-demand Multipath Distance Vector (TA-AOMDV) routing protocol that supports QoS by adapting to high-speed node mobility. In a protocol like this, a steady path assortment method is created as a path selection factor that takes into account not just node resources (accessible bandwidth, residual energy and queue length),it includes connection steadiness likelihood amongst nodes as well. The protocol also incorporates a link interrupt prediction system that alters the routing strategy established on intermittent probabilistic link steadiness estimations for adapting rapid topology changes.

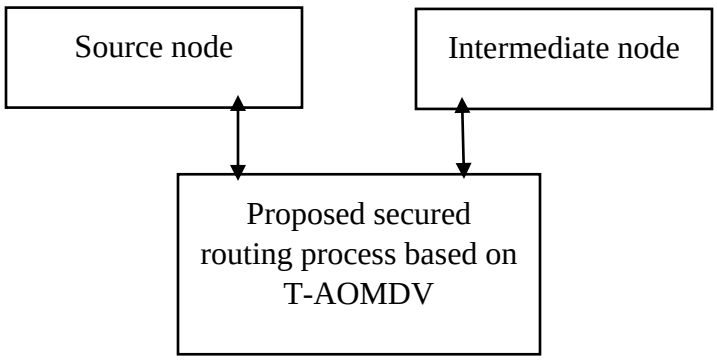
3. Research Methodology

3.1 Multipath route discovery

AOMDV routing has been utilized for finding multiple disjoint paths. Primarily, the packet success rate is calculated using random variables and variation across time to describe the data packet's in-progress success rate. The beta random variable is used to model these factors.

The route finding procedure is carried out as follows:

1. Prior to delivering a data packet to destination D, the source node S examines its route cache to see whether a path is available.
2. S will examine the available path for data transfer if there is one.
3. Otherwise, S sends to destination D a RREQ packet via intermediate nodes (Ni).
4. Ni refreshes the route cache in a routing table with information related to source, sequence number, destination, previous hop node and success rate of packet when it receives RREQ.
5. If the node is D, Ni transmits the RREP or re-broadcasts the RREQ to its neighbours in either way. This procedure continues until RREQ reaches D.
6. For each RREQ received, D unicasts the RREP packet in reverse direction towards the direction of source.
7. When a Ni receives an RREP, it changes RREP's next hop cache and then unicasts RREP utilizing already kept preceding hop node data. This process is continued until RREP reaches the value S.
8. S further uses the information from RREP to calculate the path's end-to-end success rate of packet.
9. S chooses an optimal path with a high packet success rate as a primary way. This is an optimum method for data transmission amongst S and D. As a backup path, a path with the next highest packet success rate is picked (alternate path). Figure 1 depicts the suggested block diagram.



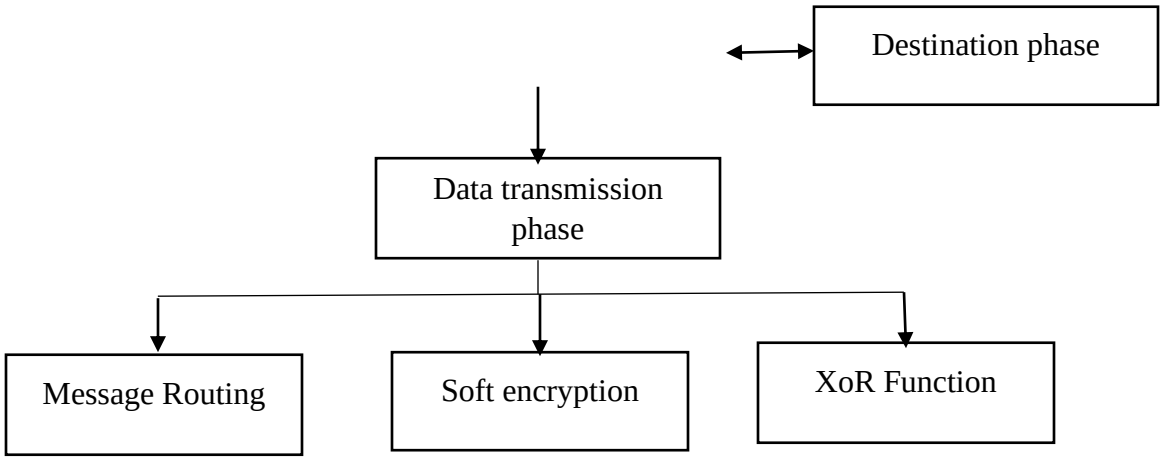


Figure.1 Block diagram of proposed secured routing process

1. Route request phase

If the packet's list of intermediate nodes is a superset of the routing table's elements, a packet is refused. Otherwise, node modifies the packet and rebroadcasts it with its own entry. When the identical RREQ is received from node b, the intermediate node discards it. When a node attains RREQ, it adds its address to route list, self-certifies it and rebroadcasts it. Conversely, Node d gets RREQ from nodes a through b and discards them from node e. Node d checks its self-certificate SCera after receiving RREQ from node a.
If it's valid, node d replaces SCera with its SCerd, removes node a's signature and signs the RREQ message with its Kd.After that, it adds its address to route list and broadcasts it once more. Figure 2 depicts an intermediate node that gets RREQ from source S directly.

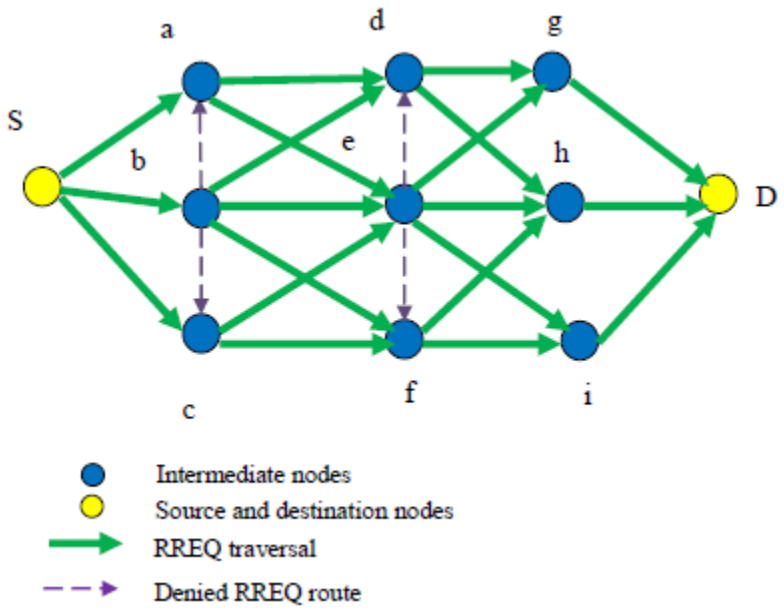


Figure.2 Route discovery

2. Route reply phase

The destination D finds several pathways –node disjoint paths and primary path – when it gets RREQ from its neighbouring nodes from every incoming route. The destination validates entire signatures and caches the route list upon receiving the first RREQ transmission. It creates a route reply (RREP) packet by decrypting and storing the session key from S. RREP is made up of the same cumulative route as RREQ, a D digital signature on whole message and also an encrypted session key. Subsequently RREP is transmitted back through a inverse route specified by RREQ's cumulative path.

Every transitional node in cumulative route verifies its own identity including the predecessor and successor nodes IDs. If both tests pass, transitional node marks the RREP and transmits it to subsequent node in the path and RREP arrives at source node consequently. This node checks to see if it got a message from its neighbour and if that neighbour is the path's initial node. If the entire signatures are confirmed, the route is then approved as legitimate. The session key from destination is also decrypted and saved. If a destination obtains an identical RREQ, it checks the RREQ's path against its route cache. Only when the nodes of source and destination are identical, a path is a node-disjoint path or else the RREQ is disregarded. A trust-defined approach is used to pick routing pathways from a collection of options.

3.3 T-AOMDV based secured routing process proposed

This stage employs a trust mechanism as well as a secure routing procedure that employs a unique node disjoint AOMDV routing process.

1. Trust mechanism: The trust system has been based on ideas presented in [10, 11], which advocate for detecting malicious nodes by node activity and packet observing, then utilizing such information for either enhancing or decreasing trust rating of nodes. A node keeps an eye on each neighbouring node to whom it transmits packets and it increase or decrease the nodes trust value based on the node’s behaviour it has acted responsibly or not (i.e. positively transmitting a packet) or poor behaviour (i.e.failed to transfer a packet and has failed in doing this operation). The trust value of a node will rise quicker, while there are a lot of positive continuous packet transfers. The node’s trust value will fall quicker, while there are a significant number of failed continuous packet transmissions. As a result, both good and bad nodes will be rapidly identified.

A node's trust value is computed as follows: $Wd * Td + Wr * Tr = Tn$

Where Wr and Wd are weights for trust suggestion Tr and direct trust value Td respectively. In case of several positive continuous packet transfer times, $Td = Td + cTs$ and in case of numerous failed continuous packet transmissions, $Td = Td – cTf$. Ts denote the total number of positive transfers and total failure transfer times are denoted by Tf in subsequent equations, while c is a constant number.

The packet success transfer time TS is raised by one when a packet is positively transferred and TS is reset to 0 and Tf is increased by 1 for unsuccessful transfers. Throughout the AOMDV packet forwarding operation, these values are determined by keeping an eye on the nodes around.

For instance when packets from node A are transmitted to node B, amount P = P B(B,A) / P A(A,B) may be calculated, where P A(A,B) denotes packets quantity passed by node A to node B. PB (B,A) is packets quantity that node A has sent to node B. If P is more than 95%, an attack on the packets has occurred and Tf is raised by 1. Ts are reduced by 1 if this is not the case. The trust values table (also known as trust table) for each node is found by means of the packet from AOMDV HELLO message. Once a node gets a neighbor's HELLO message, it obtains trust table and compares it to its own trust table to see if the two tables contain any shared nodes. The recommendation calculation operation is initiated while a node is keen to accept the packets that have been sent with Tr computed as in equation 1:

$T_r = \sum_{X=0}^{n} 0.1 * T_{D(A \rightarrow X)} * T_{D(X \rightarrow C)} / n$ ……..(1)

Tr is computed whenever a node requires to transfer a packet, or else the same is saved and regenerated while the node gets one more HELLO message. Assuming that node A wishes in transferring packets to node C and X has a shortest trust relationship with C is 7.Tr = 0.1*8*7=>5.6, is the trust recommendation assessment taken from the similar table when node A's shortest trust in node X is at a value of 8.

2. Secured routing process: The following is how the unique node-disjoint AOMDV protocol is built.To recognize a destination node, a RREQ message is broadcasted by a source node during AOMDV protocol's routing discovery phase. An intermediate node analyses the packets' path accrue list including the hop sum from source to itself once it receives an RREQ message. Once an intermediate node receives an initial RREQ message, hop count gets recorded as its lowest number and with a reverse route database, sets up a reverse route to a node that broadcasts RREQ. The hop count is evaluated and selects the count with fewest hops, when an intermediate node obtains two RREQ messages.

After that, the reverse route table will be reset by a reverse route. If the total number of hops is identical, an intermediate node records a same hop count in reverse route database. Once destination node receives a RREQ message, it starts routing reply operation and sends a RREP message to source node. Once an intermediate node obtains a replacement RREP message and sends a RERR message to a node that transmits a RREP message, the route gets broken. A secure routing protocolutilizing this AOMDV in a node-disjoint manner is briefed below:

To locate a destination node, a source node sends out an RREQ message utilizing node-disjoint AOMDV protocol described above. Once a potential destination node is identified and RREQ is received, a reply RREP message is sent. Every intermediate node will check the trust value in RREP reserved column to a neighbouring node's trust database for determining the correct trust value, so as to use while transmitting RREP message on its way to destination node. The reserved column's trust value gets substituted by neighbours

node's trust value once the reserved column's trust value is larger than neighbours node's trust value. The trust value of reserved column will be left intact and a packet will be sent to subsequent intermediate node on the path. The source node arranges routes according to their trust values after receiving each RREP message and their trust values, then splits data into three parts indicated above and encrypts it by means of XOR operations in Equations (2).

A’ = A XOR B XOR C = AXOR C, B’ = B XOR C’ ……..(2)

The data will subsequently be sent to appropriate routes by source node dependent on the data's secrecy level. If a chosen path is not suitable for transmitting all or part of the data throughout this process (due to an insufficient trust value), a routing procedure will be restarted.

3. Route maintenance: A route error is reported to source by node's neighbours when a route is disrupted due to node mobility. A source will delete the route from routing database consequently. It is possible for a source to use another way to the destination. If a source is not comprised of any record for destination and when the session is still running, a new route discovery is commenced. This approach uses a nonce in route error messages along with a digital signature for validating the packet and to confirm its freshness.

4. Message encryption and routing

The data can be sent when the best path is found. The 4n-bit message is split into four pieces of n bits each during the data transmission phase. To obtain an original message, three encrypted message parts A', B', and C' gets decoded at destination node by means of a following XOR operations indicated in equation (3)

A’ = A XOR B XOR C = AXOR C, B’ = B XOR C’ …… (3)

Algorithm for Securing T-AOMDV

Step: 1- To improve the system's security, the route finding step using RREQ and RREP is accompanied by a digital signature.
Step: 2- Self-certificates and session keys are used to sign RREQ/RREP messages.
Step: 3 - Depending on the path length and node trust value, a safe route selection model is recommended.
Step: 4- The data transfer phase is provided to the following route discovery.
Step: 5–The data is encrypted utilizing soft encryption and XOR operations during data transfer phase.
Step: 6- When a message arrives at target node, it is decrypted and the original message is recovered.

4. Simulation results

The simulation tool utilized in this research for securing multi path routing is ns 2.34. The following performance indicators are used to compare the proposed message security system (TAOMDV) to the benchmark scheme (denoted T-DSR): (1) Route selection time - the overall amount of time-period it takes to choose a routing path (2) Trust compromise - the overall quantity of access breaches found along all routes. The variance amid (ne) the encrypted message portions quantity received by n and Tn is the trust level of n characterized as an access violation at node n, if $n_e \geq T_n$. The equation (4) is used to determine the routing path p trust compromise.

Trust Compromise= $\sum_{n \in N_P}(n_e - T_n)$, wherever $n_e \geq T_n$. ……..(4)

The following are two simulated situations to consider:

A. Nodes quantity differs in relation to a single fixed mobility.

The extreme speed of nodes has been set to 20 m/s while the malicious nodes percentage in network is set to 10% in such situation. This analysis changes the network size for T-AOMDV and T-DSR schemes, wherein an effect of this modification on data transmission success ratio is reliant on route selection time and a trust conciliation for T-AOMDV and T-DSR schemes.

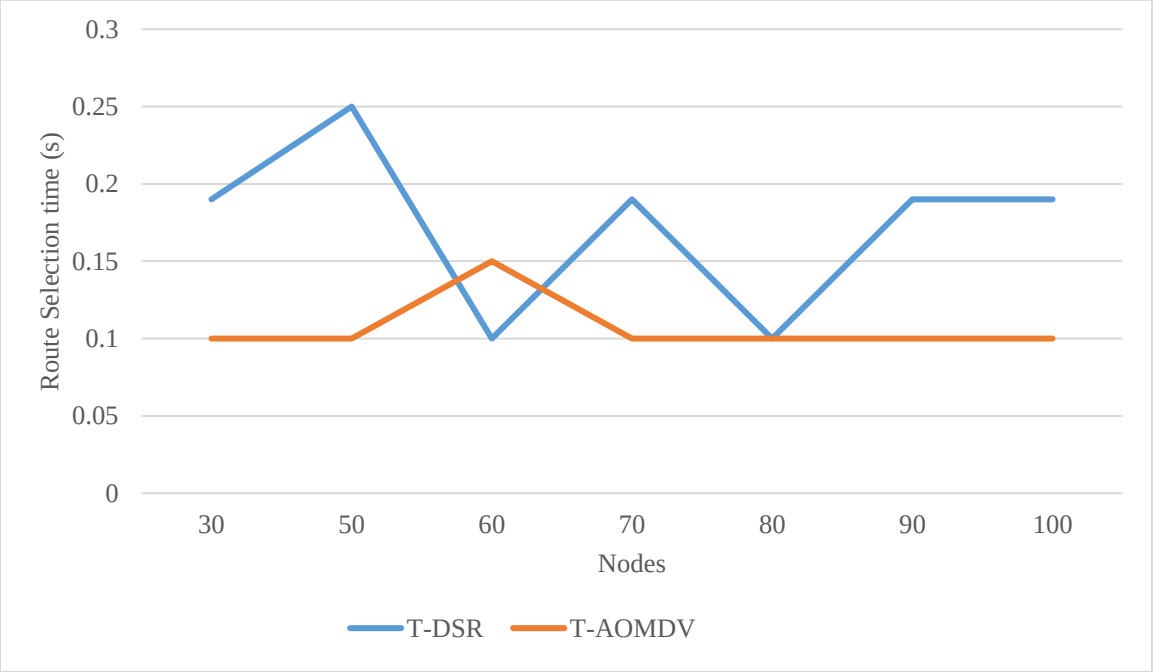


Figure 3 Route selection time

As associated to T-DSR scheme, figure 3 demonstrates that T-AOMDV scheme produces a quickest route selection time. T-AOMDV and T-DSR systems require reliable routes in message routing as there have been several instances when T-DSR scheme is unable to

rapidly find disjoint paths for routing, owing to the presence of critical nodes in identified chosen paths. While utilizing T-AOMDV scheme, this is not essential for the purpose of routing as the latter can discover trustworthy node-disjoint routes that copes through critical nodes presence. As compared to T-DSR approach, the route selection process is much quicker.

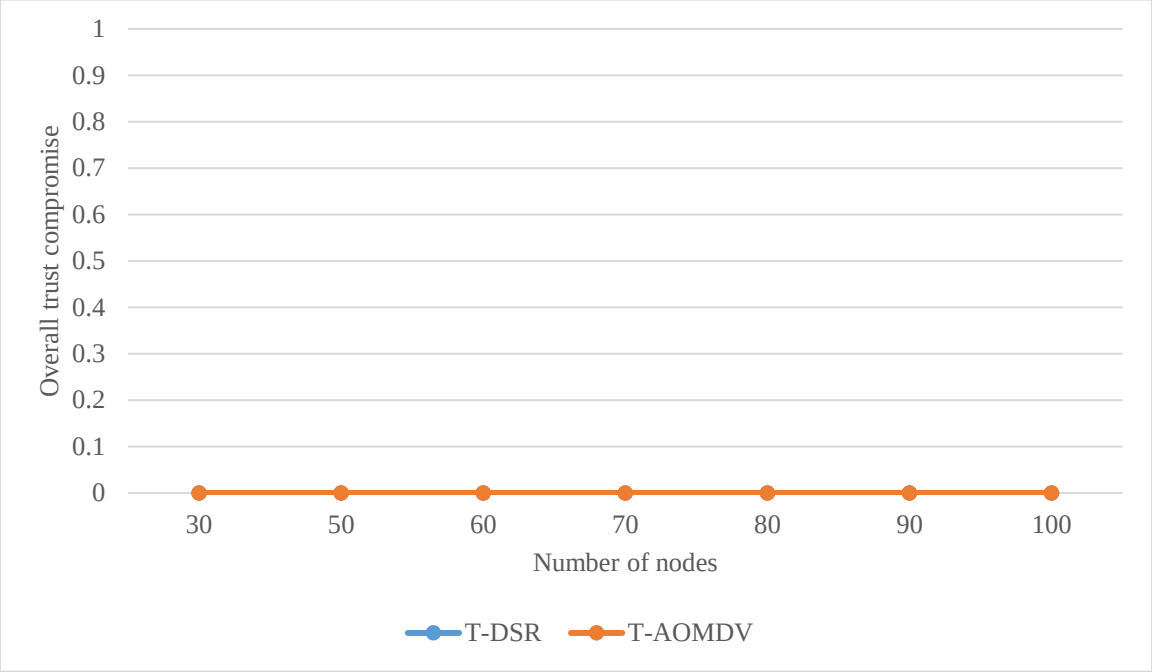


Figure 4 Trust compromise

Figure 4 illustrates that in all scenarios, T-AOMDV and T-DSR systems possess a zero trust compromise irrespective of its network size. It may be vindicated that routing pathways in both systems are chosen in such a manner, that none of the routing path's node is allowed to get additional encrypted message portions than its permitted trust level. As compared to TDSR and T-AOMDV schemes and in systems that do not deal with security limitations, trust values are allotted to nodes at random as well as those in defined routing paths (like AOMDV and DSR). As a result, these methods produce minimal message security.

B. Malicious Nodes quantum is varied with single Fixed Mobility and single Fixed Number of Nodes

This is where the mobility situation is set in stone. The total number of nodes is set at 90. Malicious nodes come in a variety of sizes. Figures 5 and 6 show the effect of its change on trust compromise and route selection time related to T-DSR and T-AOMDV systems respectively.

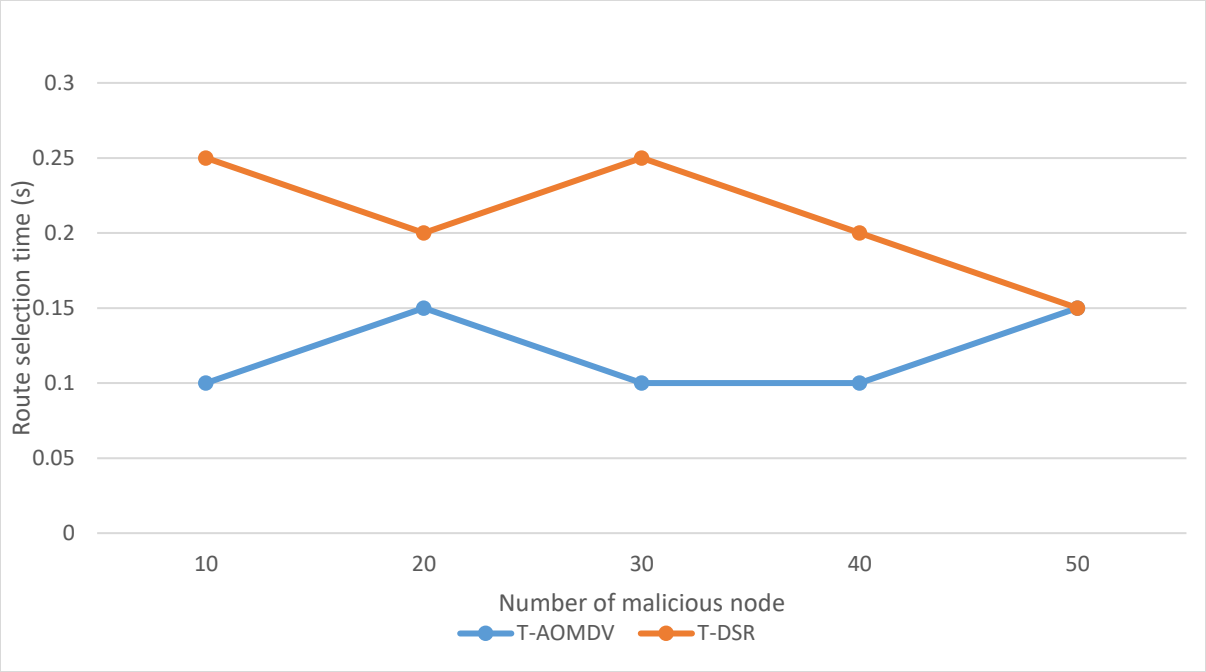


Figure 5 Malicious Nodes based Route selection time

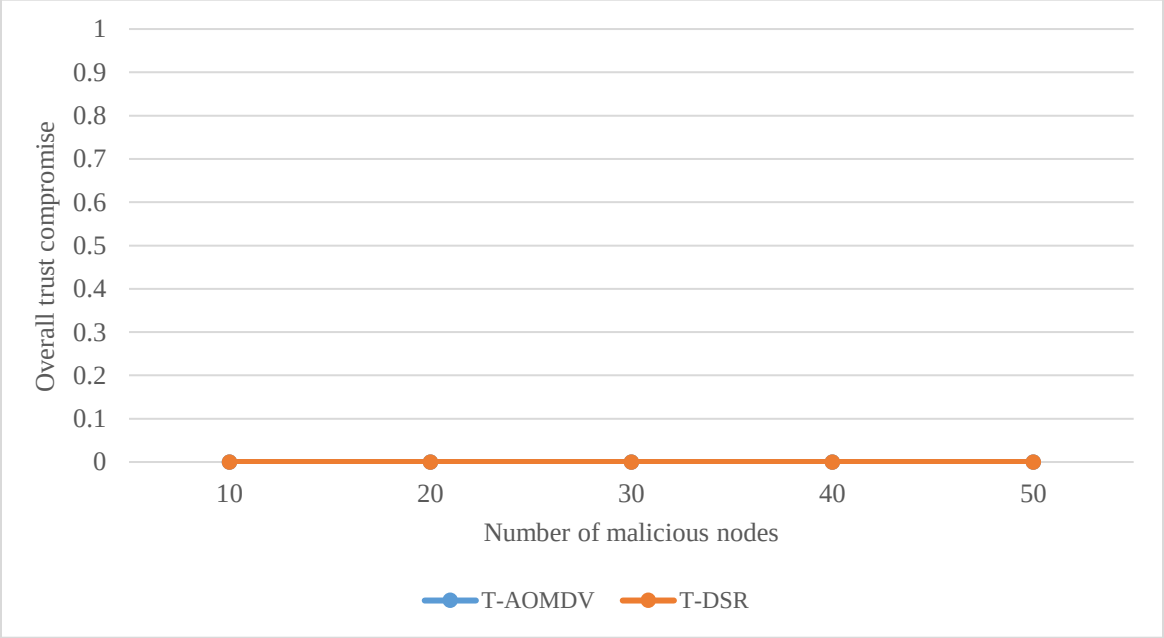


Figure 6 Malicious Nodes based Trust compromise

The T-AOMDV method takes a smaller amount of time than T-DSR scheme to ascertain the path set towards routing as shown in Figure 5, irrespective of the fraction of malicious nodes.

This might be because the targeted trust model in this situation has the capacity to modify the trust calculation process, resulting in a rapid selection of trustworthy nodes in chosen

routing route.Figure 6 shows the same results as Figure 4, namely the trust compromise related to T-AOMDV and T-DSR is zero in entire cases.

5. Conclusion

Multipath routing methods give protection against malicious nodes that collaborate.Secure Multi-path Routing is a full multipath protocol which determines every prevailing node-disjoint routes up to a specified maximum number of hops. Secure multipath routing and data transfer for MANET are based on message security method in which digital signatures are provided with RREQ messages to improve security and the signatures are validated by destination nodes presented in this paper. Secure route discovery is performed at that time, centered on node trust value and path length. Data broadcast begins after route finding. Soft encryption and XOR procedures are used during data transfer. When the message arrives at target node, it is decrypted and the original message is recovered. A T-DSR scheme and a conventional multipath algorithms are less safe than the suggested T-AOMDV message security system for MANETs. The suggested technique will be further developed in future by comparing it to a number of existing secure routing systems.

Reference

[1] Singh, D., Sharma, B.K. and Kumar, A, "A survey on challenges in multipath routing for adhoc networks", International Journal of Emerging Technology and Advanced Engineering,
February, 2014, Vol. 4, No. 1, pp.376–381, ISSN 2250-2459.
[2] Banoth Rajkumar and Gugulothu Narsimha, "Secure multipath routing and data transmission in MANET", Int. J. Networking and Virtual Organisations, Vol. 16, No. 3, 2016.
[3] Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat, Ting-Yun Chi and Sanjay K Dhurandher, "Multi-Path Trust-Based Secure AOMDV Routing in ad hoc Networks", IEEE, 2011.
[4] Rani Sahu, Sanjay Sharma and M. A. Rizvi, ZBLE: "Energy Efficient Zone-Based Leader Election Multipath Routing Protocol for MANET", International Journal of Innovative Technology and Exploring Engineering, ISSN: 2278-3075, Volume-8 Issue-9, July 2019.
[5] Mohammad Sirajuddin, Ch. Rupa , Celestine Iwendi and Cresantus Biamba, "TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network" , Hindawi, Security and Communication Networks, Volume 2021, Article ID 5521713, 9 pages, https://doi.org/10.1155/2021/5521713.

[6] V. V. Sarbhukan and L. Ragha, "Establishing secure routing path using trust to enhance security in MANET," Wireless Personal Communications, vol. 110, no. 1, pp. 245–255, 2020.

[7] H. Jhajj, R. Datla, and N. Wang, "Design and implementation of an efficient multipath AODV routing algorithm for MANETs," in Proceedings of the CCWC, pp. 0527–0531, Las Vegas, NV, USA, December 2019.

[8] M. Mittal, C. Iwendi, S. Khan, and J. A. Rehman, "Analysis of security and energy efficiency for shortest route discovery in low-energy adaptive clustering hierarchy protocol

using Levenberg-Marquardt neural network and gated recurrent unit for intrusion detection system," Transactions on Emerging Telecommunications Technologies, Article ID e3997, 2021.

[9] D. Sarkar, S. Choudhury, and A. Majumder, "Enhanced-Ant- AODV for optimal route selection in mobile ad-hoc network," Journal of King Saud University-Computer and InformationSciences, vol. 8, 2018.

[10] Y. Harold Robinson , E. Golden Julie, Krishnan Saravanan, Le Hoang Son, Raghvendra Kumar, Mohamed Abdel-Basset, and Pham Huy Thong, "Link-Disjoint Multipath Routing for Network Traffic Overload Handling in Mobile Ad-hoc Networks", IEEE Access, Volume 7, 2019.

[11] Mohit Angurala, Manju Bala and Sukhvinder Singh Bamber, " Load Balanced AOMDV-An Improvement over AOMDV Protocol", International Journal of Control and Automation, Vol. 12, No. 5, 2019, pp. 244-249.

[12] Jain, M., Mishra, S., and Sinhal, A., "Optimum Route Selection using Improved FF-AOMDV to Increase Network Lifetime in MANET ", International Journal of Ethics in Engineering & Management Education, Volume 5, Issue 6, June 2018.

[13] Huang, J-W., Woungang, I., Chao, H-C., Obaidat, M-S., Chi, T-Y and Dhurandher, S.K, "Multi-path trust-based secure AOMDV routing in ad hoc networks", IEEE Global Telecommunications Conference, December, pp.1–5, 2011.

[14] Woungang, I., Obaidat, M.S., Dhurandher, S.K., Chao, H-C. and Liu, C, "Trust-enhanced message security protocol for mobile ad hoc networks", IEEE International Conference on Communications, June, pp.988–992, ISSN: 1550-3607,2012.

[15] Zeyad M. Alfawaer and Belgaum Mohammad Riyaz, "An enhanced Multipath Strategy in Mobile Ad hoc Routing Protocols", IEEE, 2017.

[16] Bhagyalakshmi and A. K. Dogra, "QAODV: A flood control ad-hoc on demand distance vector routing protocol," in Proceedings of the ICSCCC, pp. 294–299, Jalandhar, India, March 2018.

[17] M. S. Hussain and K. U. R. Khan, "Network-based anomaly intrusion detection system in MANETS," in Proceedings of the ICISC, pp. 881–886, Coimbatore, India, December 2020.

[18] M. Sirajuddin, C. Rupa, and A. Prasad, "A trusted model using improved-AODV in MANETS with packet loss reduction mechanism," Advances in Modelling and Analysis B, vol. 61, no. 1, pp. 15–22, 2018.

[19] Rahul K. Ambekar and Uttam D. Kolekar, "A Survey on Multi-Path Routing Protocols In Mobile Ad Hoc Network", IIJATES, Vol-4, Issue-10, 2016.

[20] Zheng Chen, Wenli Zhou, Member, IEEE, Shuo Wu, Li Cheng, "An adaptive on-demand multipath routing protocol with QoS support for high-speed MANET",IEEE, 2017.

[21] BHAVSAR, CHINTAN, and SONAL BELANI. "PERFORMANCE COMPARISON OF PATH LOSS SENSITIVE ROUTING PROTOCOL AND MULTIPATH ROUTING PROTOCOL FOR MANETS."International Journal of Computer Science Engineering and Information

Technology Research (IJCSEITR) ISSN(P): 2249-6831; ISSN(E): 2249-7943 Vol. 5, Issue 5, Oct 2015, 43-52

[22] Malhotra, Atul, et al. "Packet Sizing for AOMDV and OLSR MANET Routing Protocols." *International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC)* 3.3 (2013): 99-104.

[23] Singhroy, S. H. R. U. T. I., P. L. Zade, and N. I. L. I. M. A. Bodhya. "Comparative Analysis of AOMDV AODV DSR and DSDV Routing Protocols for Cognitive Radio." *International Journal of Electronics, Communication & Instrumentation Engineering Research and Development (IJECIERD)* 3.2 (2013): 1-6.