International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-11 E-ISSN: 2347-2693

Multipath Optimised Link State Protocol (OLSR) with Security for Mobile Ad-Hoc Network

Madgula Vijaya Bhaskar[1*], G.A. Ramachandra[2], Y. Deepika[3]

[1*]Department of Computer Science & Engineering, Rayalaseema University, India
[2]Department of Computer Science, S.K. University, India
[3]Government Polytechnic, Dharmavaram, India

**Corresponding Author: vijaya.bhaskar2010@gmail.com*

Available online at: www.ijcseonline.org

Received: 16/Oct/2017, Revised: 26/Oct/2017, Accepted: 10/Nov/2017, Published: 30/Nov/2017

***Abstract*:** Without the dependence of any infrastructure or central administration to create a temporary network that includes a group of nodes and wireless hosts called as the Adhoc Mobile Network (MANET). Where multipath routing in MANET has been used primarily to transmit data without interruption. Everywhere, the routing technique is primarily considered to ensure the transmission of the message while being used in some protocols. But transmission security is one of the main disadvantages of this network. Therefore, use Secure Multipath Optimized Link State Routing Protocol (SMOLSR), which is a proactive approach to routing protocol-controlled tables, to improve efficiency, which primarily depends on multipoint relay selection (MPR). A new routing protocol for MANET is the progress of the OLSR, which integrates the multi-route strategy and the source routing control scheme. In this protocol, a Dijkstra adaptive algorithm (ADA) has been developed to estimate short-time path based multipath routing and create a control node using the hop in hop authentication model through the bidirectional authentication process (TWA). Initially, find a more limited path using the Dijkstra calculation to create a duplicate topology. In this way, delete the inner and third centers, look for a second more limited path using the Dijkstra calculation. This methodology is called a multi-Dijkstra algorithm. The main objective of the research work defining the quality of the link and the selection of the paths. The TWA process is performed for security to effectively transmit the message. If an interrupt occurs in the source-destination path, it automatically confirms the route to deliver the end-user message without loss of data. The transmitted message is well protected by a TWA process. The performance of the proposed SMOLSR protocol is compared with the many traditional protocols such as OLSR, AOMDV and CA-AOMDV. As a result, the results of the proposed SMOLSR protocol have surpassed that of other protocols.

Keywords **-** Multi-Point Relay (MPR), Two Way Authentication (TWA), Adaptive Dijkstra Algorithm (ADA).

I. INTRODUCTION

One of the major types of ad hoc networks is called MANET that can transfer the message according to the user's request since MANET is said to be mobile (unstable network topology) that uses the wireless connection to dynamically link the different nodes. Likewise, wireless correspondence between MANET hubs has a telecommunication nature that can offer excessive packets and generate a storm communication problem. In other words, MANETs [1] consist of many autonomous nodes often comprised of mobile devices or moving parts that can be reorganized in different ways and operate without any network administration. In addition, it is said that MANET is a point-to-point network without pre-existing infrastructures. Therefore, to improve network stability by calculating the connection quality measures used to send data packets without interruption. But this approach is not completely satisfied, the user needs in terms of video transmission because in the previous job the data communication adjusts the data speed according to the best connection between the source and intermediate or destination nodes. It will not be fully compatible when data can be data transmission, such as audio or video.

There are two types of routing protocol in MANET, such as one-way routing and multi-route routing. To improve data transmission speed and reduce latency, multipath routing in MANET was primarily used to reliably transmit data packets. Where this routing technique has been considered for secure message transmission. The multiple routing path focuses on this document which includes some issues such as node mobility that creates dynamic topology, difficulty in maintaining paths, unpredictable link properties that expose signal propagation and packet collision, problems encountered hidden and exposed terminals, the insecurity and the limited battery life of mobile devices. Communication is transmitted from source to destination using the routing protocol of multiple paths. Suppose that any of the routes fails during this communication, so you can use a backup path for efficient message transmission to destination [2].

There are three main challenges to selecting multi-route routing protocols. They are as following.

1. Path selection, where multipath can be used simultaneously for parallel data transmission
2. Discover multiple paths
3. Spread the load on multiple paths

MANET provides three types of routing protocol, such as proactive, reactive and hybrid routing protocol. The various features and capabilities of the multipath routing protocol are analyzed in this survey and illustrate the results among them. Fig. 1 represents the classification of the multipath routing protocol.

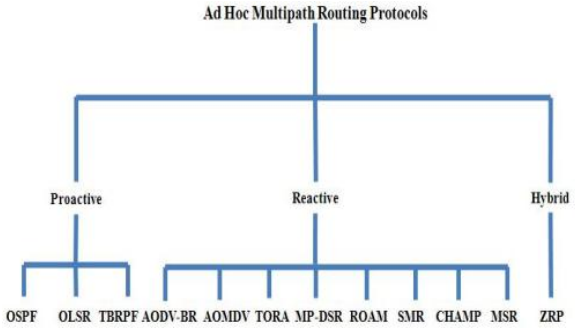


Fig. 1 Multi-path Routing Protocol Classification

This survey reviews the searched research on proactive (on-demand) routing protocol (based on tables) and the hybrid routing protocol [3]. The three multipath routing algorithms called Ad-Hoc On-Demand Distance Vector (AODV), Optimized Link State Routing (OLSR) and Zone Routing Protocol (ZRP) have been analyzed and show the corresponding advantages and disadvantages. Therefore, it has been shown that ZRP achieves better results than the other two methods. In addition, the development of the different security routing protocol mechanism and the different parameters to avoid different attacks is the main requirement in this analysis. In this survey, we analyzed the susceptibility of OLSRin contradiction to a node isolation attack [4]. A detailed type of node isolation attack suggests denial of service (DOS) attack that can be easily parsed in OLSR (EOLSR) to protect OLSR nodes from attack. Therefore, isolation attacks are detected with the help of Hello Packet to see if a node announces the correct topology information or not. This security of the EOLSR method is an important problem in this model. The hybrid routing protocol based on a modified Dijikstra algorithm [5] has introduced that allows routing in the various sparse and thick topology paths. A progressive OLSR protocol (AOLSR) is exposed in the light of the versatility of centers and the vitality of centers and connections. Proactive and reactive functions are combined to form the ad hoc hybrid routing protocol. They also introduced two cost functions, mainly to build the following paths, such as

- Link-disjoint paths
- Node-disjoint paths

Then, handle the changes in the network topology by using path retrieval and searching for cycles. Therefore, the AOLSR protocol has improved network life, scalability, reliability and confidentiality of MANET. But security through a partial network topology is the main problem in this technique presented by AOLSR.

A. Proposed Work

In this research, develop a new Adaptive Dijkstra algorithm to estimate multi-path routing based on link knowledge and create node verification using the hop-by-hop authentication model through bi-directional authentication. Typically, multipath nodes are involved in mixed and convoluted nodes and independent nodes. Therefore, the independent multipath is part of the stand-alone hub (independent node) and connects freely (regardless of the connection). The non-concentrating multidirectional uses a non-convergence basis that does not require reciprocal centers between source centers and targets. The multidirectional autonomous connection expresses that common convergence centers can exist without being shared between trade unions. The multi-path alludes to a standard that distinctive shapes share at least one connection. Multi-way blended is a blend of both types of multipath. Among these, the multiple free hub path has more autonomy, since each hub of the autonomous multiauton hub is autonomous, despite the links. Therefore, the contribution of the article is as follows,

- The introduction of the AdaptiveDijkstra algorithm in the Secure Multipath-OLSR protocol that allows multiple multipath approaches
- A bidirectional authentication process is proposed to deploy multiple security rows against attacks that improve packet data security issues while transmission is performed in the recognition path.A two-way authentication process is proposed to implement multiple lines of protection against attacks which enhancing the data packets security issues while transmission takes place in the acknowledge path.

B. Organization of the paper

- The rest of the document is presented as: Section II discusses the detailed description of related works to provide security on the attacks to MANET. Section III elaborates a description of the SMOLSR protocol proposed for transmitting the data packets to MANET. Section IV illustrates the experimental results of the SMOLSR routing protocol. Section V discusses the final results of the proposed work.

II. RELATED WORKS

Ganie and Sharma [6] presented and evaluated an efficient cluster head (CH) selection for fault-tolerant routing in MANET. Energy consumption has been reduced considering the pooling as a key routing technique. In addition, CH energy has been maximized and, at the same time, single link failure has been reduced to MANET. In addition, the useful life of the network and fault tolerance have been improved by an efficient energy pooling. A local repair method has been introduced to prevent the break from the link. Dutta and Biswas [7] suggested a new approach based on the new type of black hole attack for the AODV multipath. Here, the author of the attack focuses on the nodes through which an AOPV multipath crosses more than one threshold number of alternative paths. Such node type has been selected and launched a black hole attack where the number of routes was damaged in a single attempt. Since an attack consumes only less energy than the original black hole attack, it can be used for a long time over the original black hole..

Kumar, et al. [8] evaluated the effect of black hole attack on the MANET routing protocol. The effects were evaluated based on the study of the vulnerabilities of two protocols, namely AODV (I-AODV) and AODV improved at different pause times. Through a malicious knot, the effect of I-AODV was lower than the ODV. In addition, AODV overload has been affected twice as much as I-AODV. Therefore, it has been shown that I-AODV provides better performance and is more vulnerable to black hole attack. Similarly, other techniques can be analyzed and different attacks may be considered instead of black-hole attacks, respectively. Thomasundaram [9] offered a protocol to prevent and detect the black hole attack on MANET via the CBHDAP detection and avoidance protocol cryptographic key (CBHDAP). Some parameters such as packet delivery speed, hop count, and path response were used to prevent black hole attacks during transmission. CBHDAP performance has been validated against other protocols and have proven to have provided optimum results for all metrics, such as performance, probability detection, and end-to-end delays.

Using these parameters, the protocol may also detect several security attacks that are more likely to detect. The technique was overcome by Pavithra [10] analyzing some prevention techniques to identify the black hole attack by avoiding using asymmetrical and symmetrical methods of encryption and IDS techniques of a non-cryptographic method. Additionally, the pooling method was used to detect the attack, so the cost was also reduced successfully. Hence the prevention techniques and have been provided and discussed that various concepts used in the survey help determine the black hole attack. However, there are some drawbacks that can be overcome by another concept, respectively. Mahomaod, et al. [11] A modified AODV protocol was recommended for detecting black hole attachment in MANET. The M-AODV method was used to prevent black hole knots and to determine safe paths by maintaining trust values in each node and identifying nodes with the corresponding sequence number.

As a result, the number of packets sent and received was calculated and the nodes' reliability and reliability values were adjusted by the M-AODV protocol. But even so, performance analysis of the M-AODV protocol needs to be analyzed and developed simulations based on different security parameters. In addition, more attacks on AODV have to be focused to solve the problems of an attack. Ahlawat and Chaturvedi [12] examined black hole attacks and comparative analysis of several IDS schemes in MANET. Analysis of different schemes has been applied to improve MANET performance during the occurrence of a black hole attack. In addition, it provided a solution through the use of an IDS schema based on anomalies. The comparison was made between the existing solution in different parameters. Based on these comparisons, the packet delivery fraction has been increased while at the same time the standardized routing load has been reduced by developing an improved IDS scheme, respectively. However, the problem of black hole attack exists as an active investigation to understand several attacks and also the improved IDS development through which the shortage of presented HIV can be successfully eliminated.

Kumar and Aulakh [13] have provided clarification on the prevention and detection of multiple black holes in a network. This analysis also determined a safe way to transfer data from the source node to the destination. We have reviewed many routing protocols and research papers, ad hoc networks, and various techniques for preventing black hole attacks. Based on these reviews, it was concluded that, compared to other routing protocols, the AODV was prone to black hole attack. The work was initiated by a method of identifying the node often and an optimal result was established for detecting and preventing the black hole attack in MANET. Rather, simulation can be used to improve performance and detect the multiple attack of black holes successfully. Dubey and Barua [14] studied MANET techniques to mitigate attacks on black and gray holes. We have reviewed recent research activities in the Ad-hoc network, which included a summary of MANET functionality and features. A MANET routing field was also determined by the literature review.

The main objective of the survey was AODV and DSDV, which is the most popular routing protocol in MANET. Many improvements and variations have been proposed due to the popularity of the AODV protocol. Lei, et al. [15] The intrusion detection prevailed for the gray hole and the black hole attack. These attacks were detected by demonstrating a focus on an Ad-hoc network based on cross-layer design. We've introduced a path-based method that does not send additional audit packages and listens to the next hop action, as well as system resources to detect the node. The rate of false positives has been reduced in function of the high network overhead in a MAC layer protocol. We have estimated negative and positive impacts that have provided a

less competitive detection rate, for example, by an adaptive detection scheme. Mandala, et al. [16] investigated the severity of black hole attack and variance in wireless MANET. The compromising source node (CON), the compromising relay node (CRN), and the corruption routing table (CRT) have been some of the new security measures that have been proposed for the use of severity estimation.

In addition, for comparative analysis, the hybrid black hole was introduced with a HBHA cooperative and an independent HBHA. The new HBHA proposed was compared and it was shown that the IBHA was the most serious attack of CHBHA. Therefore, CHBHA was one of the most effective attacks against the other. However, security prevention must be developed and the severity of these attacks should be considered in order to achieve effective and effective preventive measures accordingly. Adnane, et al. [17] described the contributions and security techniques based on trust in OLSR. Through the use of the reliability specification language, a trusted OLSR analysis was presented and demonstrated the responsibility of its reasoning that allows each node to calculate the behavior of other nodes. Then, countermeasures and prevention solutions resolve inconsistencies. even malignant nodes were casually countered. It has also been applied to other protocols in the self-organized and spontaneous environment. In addition, explicit confidence values can be used for formal analysis of protocol vulnerability correction.

Maurya, et al. [18] assessed the FSR, DSR and OLSR performance measurement using a random reference mobility model. Performance was evaluated based on average jitter, end-to-end delay, performance, and packet delivery speed. Through these comparisons, it has been shown that OLSR has provided the best performance against end-to-end instability and delay. For this instance, RTD overload and TTL-based hop count could be used for higher performance. Kaur, et al. [19] evaluated the performance of ZRP, OLSR and AODV routing protocols under Black Hole attack in MANET. These routing protocols have been calculated using various performance metrics such as jitter, end-to-end delay, packet delivery ratio, and performance. Through these parameters, it has been shown that AODV was the best routing protocol in the presence and with black hole in ZRP and OLSR in all cases. You can also focus on the prevention and detection scheme by using a particular type of security algorithm. Singh and Singh [20] suggested a black hole attack effect on OLSR, AODV and ZRP in MANET. Where the effect was analyzed by three different categories, such as hybrid routing protocol, proactive and reactive. Research concluded that the effect of black hole attack was more on AODV than others under end-to-end delay metrics, performance, and packet delivery ratios. Other security algorithms should be developed on this protocol to avoid black hole attack, respectively.

Therefore, current protocols have provided the following limits, such as network life, error tolerance, data transmission speeds, attacks, and end-to-end delays.

III. PROPOSED WORK

This section discusses the implementation of the Secure Multipath Optimized Link State Routing (SMOLSR) protocol implementation, based on Two Way Authentication (TWA) Dijkstra's Algorithm (ADA) Requirements to perform robust data packet transmission across MANET in accordance with the mobility node. The workflow of the proposed SMOLSR protocol is shown in Fig. 2.

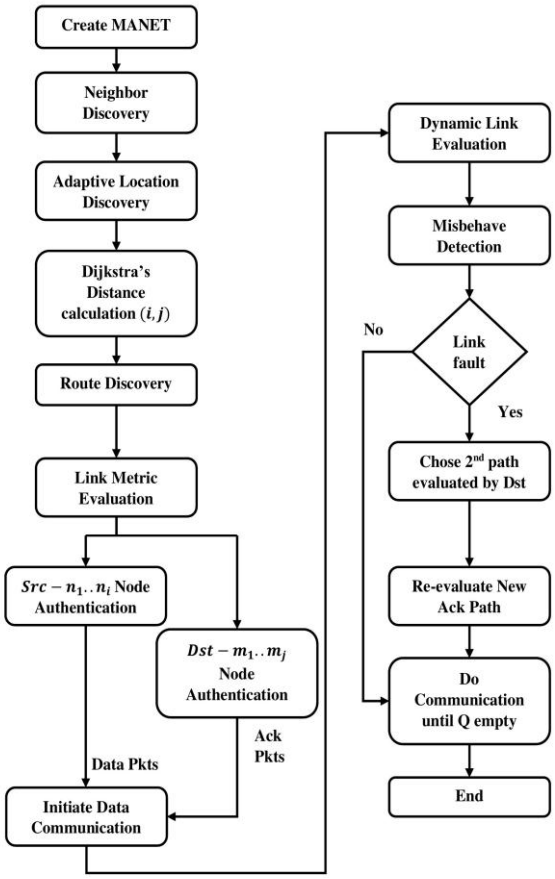


Fig. 2 Proposed SMOLSR protocol Workflow

The proposed MANET architecture formulation initially requires mobile selection by sending a request message to neighboring mobile nodes on the basis of adjacent discovery. Often, the location adaptive discovery performs a complete analysis of the location of each mobile node within the target field. After obtaining the nearby discovery details with the corresponding position, ADA is executed to find out the shortest distance (distance) between nodes (i, j). The path discovery technique that is dealt with by exploiting a routing table that accordingly selects for the evaluation of the data

rate for the particular node involved in that particular route. Then, the metric evaluation of the connection is performed by the number of nodes that join or abandon and the connection power is estimated. After gaining profitability over the transmission of data packets, source and destination nodes are evaluated for authentication. Nodes are authenticated by the TWA process via the hop-by-hop authentication model. When transmitting data packets, the source node describes the number of nodes to be transmitted based on the authentication of the source node. Then, the recognition packet is transmitted based on the destination node authentication process that sends the node detection m_j. These data and confirmation packets are used to start data communication. Subsequently, detecting any incorrect behavior in the dynamic link evaluates the states that indicate the connection error. If there are link errors, automatically select the second destination node path because the status of the link is evaluated. Then, recalculate the new state of the access path used for data transmission until Q is empty. Otherwise, continue to transmit data uninterruptedly. Table I represents the list of notations and description.

TABLE I-NOTATIONS AND DESCRIPTIONS

List of Notations	Descriptions
H	Hash function
Q	Prime number
P_u	Public key
Sig_M	Signature based node
P_i, P_r, P_t	Idle, receiver, transmitter of the power
T_i, T_r, T_t	Idle, receiver, transmitter of the time

A. Creation of MANET

The Multi-hop networks, which are used to forward the packets to the other communication nodes in succession through intermediate nodes. Some of MANET's features are summarized as follows:

- Dynamic network topology
- Nodes can perform the roles of both hosts and routers
- Limited physical security
- Channel limited bandwidth and power limited to nodes

These are the features that make MANET communication very difficult because the paths connecting the source nodes to the destination are unstable. Therefore, dynamically connect the nodes arbitrarily to establish more than one route between source and destination. Therefore, the OLpath Multipath protocol is used in MANET

B. Multi-Point Relay (MPR) Selection

The SMOLSR protocol proposed depends on the concept of multipoint relay because it decreases the degree of moderate control messages rather than articulating all the networks to complete the general centers, and even a hub informs only connections with its neighbors are said to be chosen are multipoint relays . There are two ways to select MPR for each node is described as, before, each node chooses its finished MPR as specified in the SMOLSR. It is represented as everywhere there is an adaptation in the neighborhood of a jump or two jumps. After that, knowing the available bandwidth of its neighbors and neighbors of two jumps, any node chooses its MPR to reach each next two jumps along a maximum bandwidth path. In the event that a neighbor of two jumps, there are some missed neighbors who succeed, you will choose the one with the most remarkable center.

This selection of MPR is called as everywhere there is an adjustment in the one or two jumps. Also, when the transmission capacity of a hub is accessible essentially chosen as diminished or when the transmission data accessible adjacent to a hub not selected as fully expanded. Then learn the next information and corresponding position information.

C. Neighbor and Location Discovery

The main purpose of the discovery is to discover local topology information that quickly finds the direct connection to the loss and discovery of new neighbors. Because of the loss of data packet loss. Each node in the protocol collects information about its local neighborhood from the broadcast message that receives it. After completing the adjacent discovery, the scanned data packets are the main source of adjacent nodes for system monitoring. So, he collected the neighbors that need to be selected. In complementary mode, nodes are successfully transmitted and receive data.

The best goal of Adaptive Location Discovery ALD is to minimize overhead control packs. Locating the adjacent location involves protecting networks from challenging nodes by authenticating a neighbor's location to improve safety, efficiency, and performance in MANET routing. Therefore both static and mobile environments are suitable for fast and permanent swapping of all neighbors and allow any node to validate the location. Then, the neighbor and the positions are identified to find the path effectively.

D. Route Discovery

E. The SMOLSR protocol is a proactive routing protocol to enable mobility nodes in a MANET. The stability of the link state algorithm inheriting the protocol. The OLSR protocol is an optimization of a pure link state protocol and is an essential protocol for the discovery of the path. The main purpose of the routing protocol is to find the minimum and minimum number of jumps, from a router to all possible destinations. Mobile wireless LAN is the requirement of the classic connection status algorithm to fit. The key concept used in the protocol is that of multipoint relays (MPRs). MPRs are the selected nodes that transmit broadcast messages during the flood process.

F. The routing protocol's main contribution is the number of nodes increased by reducing the communication overload and

the size of the control packets. Consequently, the protocol significantly reduces the overload of the message when compared to a classic flood system. This way, each hub retransmits the message when it gets the original message format and reduces overload issues.

G. In SMOLSR, interface status data occurs only when hubs choose MPR. All in all, you get a second optimization by limiting the number of overloaded control messages in the system. As a third improvement, an MPR concentrator can only signal connections between itself and its MPR switches. Consequently, unlike the classical link state algorithm, the halfway status data is assigned to the system. This data is used to calculate the path and the routing protocol provides the optimal path (in terms of number of nodes). Therefore, the protocol is suitable for large and thick networks as the MPR strategy works wonderfully in this specific situation.

H. Adaptive Dijkstra's Algorithm

The new Adaptive Dijkstra's Algorithm (ADA) proposal is used to estimate the shortest path between source and destination and also to reduce the price of the route. The multipath routing protocol executed the Dijkstra algorithm to find the shortest path and no disjoint path. Consider the nodes as,

G= (N, L) (1)

Where N represents the group of nodes and L represent group of links.

The main contribution of using ADA is to acquire multiple routing paths to deliver the message. In this algorithm, path disjunctions routes or dissociated node routes are recovered by adapting the different cost functions. Therefore, packets are sent from source to destination through the use of a secondary source routing mechanism (search for sources with route recovery) in the network. Fig. 3 is the topology of the network.

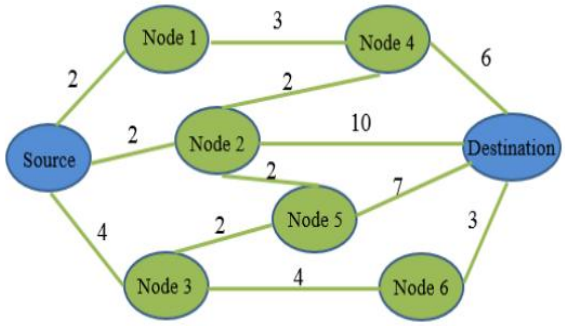


Fig. 3 Network Topology

In Figure 3, the different weight values are assigned between the source and destination path. The algorithm proposed to find the shortest path, that is, source → node2→node4→destination. Subsequently, the entries of the corresponding node are deleted in the routing table by the adjacent matrix. Then, skip node 2 and node 4 to get the second shortest path that you define with the help of the remaining nodes, respectively. Therefore, they establish the shortest path that is source → node3 → node6 → destination, respectively. These observations clearly indicate that node 3 and node 6 have been deleted in the routing table. Then, the remaining nodes derive from the same process until they reach the target node. After verifying that all paths have been verified using the Dijkstra algorithm to efficiently represent the shortest path between nodes. Then, evaluate the link stability according to the two categorizations,

• merge / departure number
• Accommodation power

The number of connections or exits from mobile nodes in the network is based on the particular field selected. If you exceed the area limit, the mobile nodes will automatically be left in the topology. The energy consumption of each of the nodes can be calculated using the equation:

$Re_{m,n} = [(Pi_{m,n} \times Ti_{m,n}) + (Pr_{m,n} \times Tr_{m,n}) + (Pt_{m,n} * Tt_{m,n})]$

(2)The algorithm to find the shortest distance path is as followed.

Input:$Pi_{m,n}$, $Ti_{m,n}$, $Pr_{m,n}$, $Tr_{m,n}$, $Pt_{m,n}$, $Tt_{m,n}$
Output:D_{μ}
Step 1:*Select node m, n*
Step 2: *Estimate remaining energy function for each node*

$$Re_{m,n} = [(Pi_{m,n} \times Ti_{m,n}) + (Pr_{m,n} \times Tr_{m,n}) + (Pt_{m,n} * Tt_{m,n})]$$

Step 3: *Calculate overall energy*
$E_{m,n} = Ei_{m,n} - Re_{m,n}$
Step 4: *Find the total energy consumption*
$EC = T + [1 / Re_{m,n}] + [1/ No\ of\ Hops]$
Step 5: *Initialize the cost of the selected path*
c (p,q) = link cost from node p to q
Step 6: *Initialize the least cost path among the set of nodes*
NN' = {α}
Step 7:
for all α nodes
if (μ) adjacent to(α)
then DIST(μ) = c(α, μ)
else D(μ) = inf
Step 8:
for check,
Step 9:
find (β) not in NN' such that D(β) is a minimum and add β to NN'
Step 10:
update D(μ) for all (μ) adjacent to (β) and not in NN' :
Step 11: *Calculate the shortest distance path*
D(μ) = min(D(μ), D(β) + c(β,μ))

Initially, select the nodes used to pass the data packets from the initial user to the end user. Then, determine the use of the host power between the selected nodes to reduce the energy consumption waste. Then, get the total energy of the selected nodes based on the difference between initial and retentive energy. Next, determine the energy consumption and cost of the node connection. This information is very useful for assessing the shortest distance between nodes. Finally, evaluate the shortest distance between neighboring nodes.

I. Two Way Authentication

The main objective of the proposed TWA model is to provide security to data packets during the transmission period. The authentication process is performed in two ways, for example

- Authentication of the source node
- Destination node authentication

The TWA method is used to provide security and deliver the message within the time period between the user and the beneficiary based on the authentication process. At the initial stage, the source node detects the adjacent node and traces the communication network that is called as route 1. Then, the second phase, the destination node to find out the nearest adjacent node, and then call route 2 respectively. If there is an error in route1, select route2 to transfer data packets within a fraction of the delay. From that case, the data packets will be delivered over time without loss of packets. The node matching algorithm and authentication algorithm are as follows:

Input *: Number of Nodes (N) Node State*
Output *: Check Authentication*

Begin
*E[i] := floor(abs(sin(i+1)) * (N_{id})^{32}*
Begin
For all Neighbors
$H_k = H(E + Q)$
For Each Packet
$Sig_M = H(H_k, P_u \| N_{id})$;
End
End
If slot = true
Check Weather Sleep or Active
If Active
Update location
//Check Authentication
Verify the signature
End
If *verification is successful*
Forward the signed broadcast package
Else
Discard the package and report to BS

Initialize the number of nodes and node status information. For all Ns, the secret key will be generated by selecting a random integer from the sender (yes). Subsequently, the hash-based key cryptography is performed to avoid data packets with the id of the corresponding node. Then, start this process for all neighbors until Q comes empty. Signature verification is under the hash key, the public key with respect to node identification. After verifying whether the corresponding node is active or the sleep mode. If you are in active mode, update the location of the adjacent node and verify the signature. Then, he transferred the signed transmission packets to the destination node. If you are in sleep mode, discard the packet and report to the BS.

J. Link Fault Evaluation

Dynamic link failure assessment is performed in this research work, which is used to identify any malicious behavior that occurs in the network link. In the absence of a connection error, it proceeds directly to the communication process until Q is empty. In case of presence, automatically choose the second path to execute the transmission process. Subsequently, re-evaluate the new Ack route to transmit recognition information through the connection and run the communication process. Eventually, it reaches the empty Q, the communication process ends.

IV. RESULT & EVALUATION

A. Simulation Model

The simulation model is the proposed performance evaluation of the SMOLSR protocol and is referred to as two different consequences, such as simulation time and attack rate. The routing protocol transmission time and the data transmission security are evaluated in this section. Table II represents the MANET simulation parameters and their corresponding values.

TABLE II-SIMULATION PARAMETERS

Parameter	Values
Total number of nodes	50,100,..,300
Simulation Time	100s
MAC Protocol	802.11Ext
Simulation Area	1200 * 1200 m^2
Routing Protocols	OLSR,AOMDV, Proposed SMOLSR
Mobility Model	Random way point
Packet Size	128,256,512,1024 byte
Transmission range	200m
Traffic Type	CBR
Attacker Nodes	10% of total nodes

B. Performance Metrics

The four different performance metrics are used for evaluating the proposed SMOLSR protocol performance are as follows:

1) Packet Delivery Ratio (PDR)

The PDR is delimited as the distributed amount of data packets to the successful node that is separate from the total number of packets received from the source node [21]. If high data packets are delivered, it is indicated that it reaches the maximum protocol performance. It is calculated as,

$$PDR = \frac{Distributed\ data\ packets}{Overall\ the\ data\ packets} \times 100 \quad (3)$$

2) End to End Delay

The end-to-end delay [22] per packet is delimited as the normal time needed to globally transmit the message to reach the destination node from the source node. Queue delays, MAC retransmission delays, buffering, propagation, and transfer time are considered delays. Therefore, it is calculated as,

$$EED = \frac{\sum_{i=1}^{n}(D_i - S_i)}{n} \quad (4)$$

3) Energy Consumption

Energy consumption is delimited as the total amount of energy used in general by the network node within the execution time. This metric is used to derive the energy level of each node in the network. It is calculated by

$$E = \sum_{i=1}^{n} E_i - Re_i \quad (5)$$

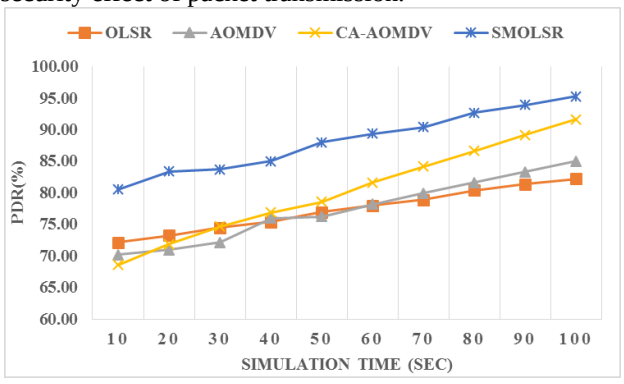
4) Throughput

The performance [23] is demarcated as the total number of bits transferred and received successfully in the receiver per unit of time. It is expressed in terms of kilobits per second.

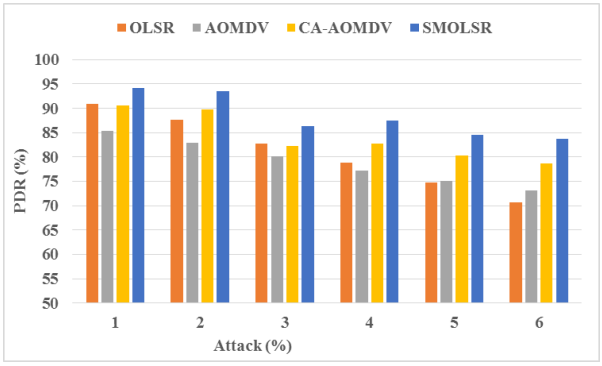
V. EXPERIMENTAL RESULTS

A. Packet Delivery Ratio

The proposed routing protocol PDR value is linked to traditional routing [24] such as OLSR, AdHoc On-demand Multipath Distance Vector (AOMDV) and Channel Aware-AOMDV (CA-AOMDV). Fig. 4 (a) represents the transmission relation of the packet. Fig. 4 (b) represents the security effect of packet transmission.



(a)



(b)

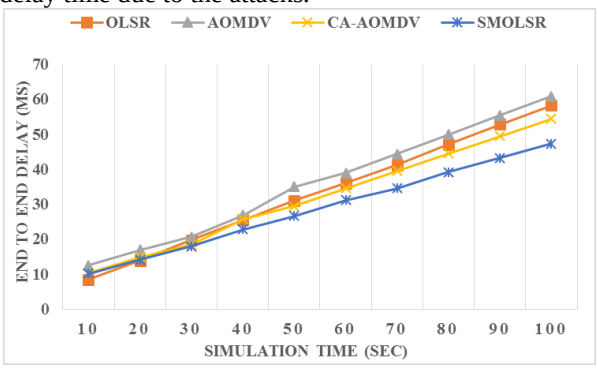
Fig. 4 Packet Delivery Ratio (a) simulation time (b) percentage of attack

From Figure 4 (a), it is clearly demonstrated that the proposed SMOLSR protocol is compared with traditional techniques. Therefore, the experimental time is between 10 and 100 compared to the packet transmission ratio. If the simulation time increases, the PDR also increases automatically. Existing OLSR, AOMDV, CA-AOMDV produced 72%, 70% and 68.54% PDR for 10 seconds and 82.15%, 85%, and 91.62% PDR for 100 seconds, respectively. Therefore, the proposed SMOLSR reaches 80.48% PDR for 10 seconds and 95.21% for 100 seconds.

From the figure. 4 (b), the attack rate ranges from 1, 2, 3, 4, 5 and 6 to PDR. The proposed SMOLSR protocol reaches 94% of PDR in the 1% attack and 83.76% of PDR in the 6% attack, respectively. Therefore, 4% of PDR improvement over the existing protocol. Therefore, the proposed SMOLSR protocol achieves higher performance than existing ones because of the selection of strong and short paths. These routes are selected to transfer data packets without reducing packet information.

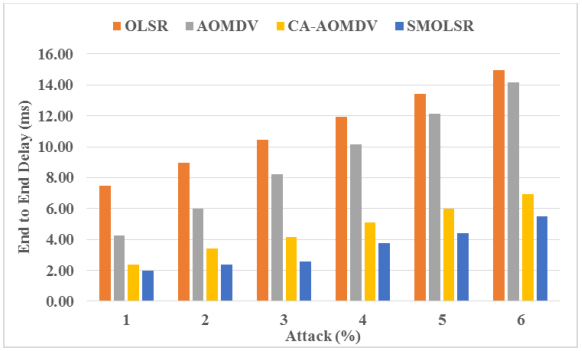
B. End to End Delay

Figure 5(a) represents the end-to-end delay with varying the simulation time for the OLSR, AOMDV, CA-AOMDV, and the SMOLSR. Figure 5(b) characterizes the end-to-end delay time due to the attacks.



(a)

From Figure 5 (a), obviously the expressions that the end-to-end proposal are delayed to variations in simulation time as 10, 20, 30, 40, 50, up to 100 seconds. If the simulation time increases, EED increases. The current OLSR, AOMDV, CA-AOMDV produced an E2E delay of 8.45 ms, 12.47 ms, 10.21 ms in 10 seconds of simulation time and 58.23 ms, 60.84 ms, 54, 33 ms per 100 seconds of simulation time, respectively. Then, the proposed SMOLSR protocol reaches 10.14 ms of EED in 10 seconds of simulation time and 47.28 of EED in 100 seconds of simulation time.



(b)

Fig. 5 End to End Delay (a) simulation time (b) percentage of attack

From the figure. 5 (b), it has been clearly observed that the percentage of attacks varies from 1, 2, 3, 4, 5 and 6 to EED. The proposed SMOLSR protocol reaches 1.97 ms of EED in attack of 1% and 5.50 ms of EED in 6% of attacks respectively. The proposed SMOLSR protocol produces better results than the existing protocol. Therefore, the proposed protocol requires a minimum time to transfer data packets over the network due to the selection of stable and short paths.

C. *Energy Consumption*

The energy consumption of the proposed protocol is derived through the simulation time. Figure 6 represents the energy consumption of OLSR, AOMDV, CA-AOMDV, and the SMOLSR.

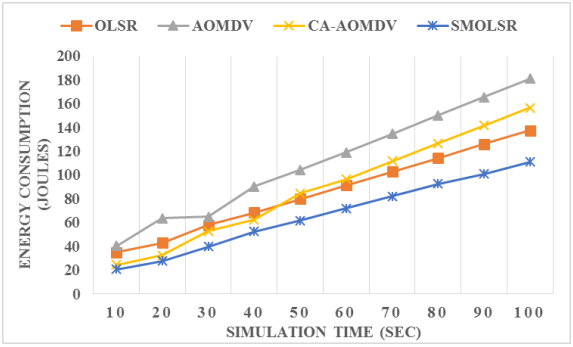
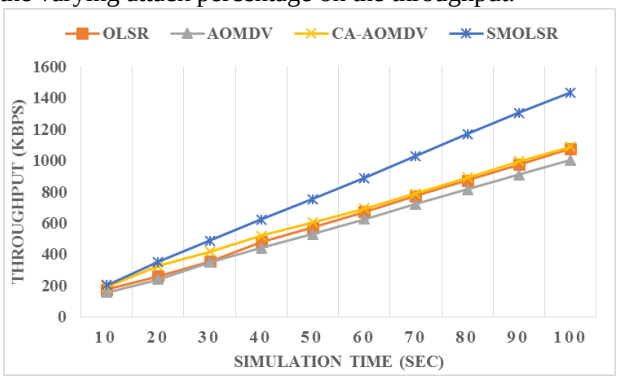


Fig. 6 Energy Consumption

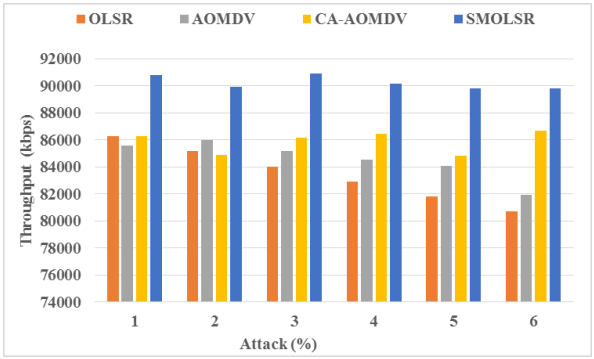
From the diagram, it was clearly observed that the proposed SMOLSR protocol with simulation time variation 10, 20, 30, 40 ... 100, respectively. For 10 seconds, OLSR, AOMDV, and CA-AOMDV existing protocols consumed 35 joule, 40.21 joule, 24.36 joule, and 20.46 joule. For a maximum of 100 seconds, protocols consume 137 joule, 181 joule, 156.66 joule, and 111.16 joule respectively. Therefore, the proposed SMOLSR protocol allows better power consumption than existing protocols.

D. *Throughput*

Figure 7(a) represents the varying simulation time on the throughput for the routing protocols. Figure 7(b) represents the varying attack percentage on the throughput.



(a)



(b)

Fig. 7 Throughput (a) simulation time (b) percentage of attack

It is clear from the figure that the proposed SMOLSR protocol produces better performance results than existing OLSR, AOMDV, and CA-AOMDV protocols. If the capacity of the discovered path can be very strong, stable and short, performance will be maximized. Therefore, loss of lost packages will be minimized in the SMOLSR protocol as much as possible.

VI. CONCLUSION

In this paper, we propose a new multi-path routing protocol known as SMOLSR to transmit data packets securely to effectively reach the end user. The Adaptive Dijkstra algorithm proposed and the two-way authentication process called the ADA-TWA algorithm to successfully determine the shortest path and send the message between the source destination node with secure transmission. Various performance measures such as end-to-end delay, throughput, packet delivery ratio, and energy efficiency are used to test the effectiveness of the SMOLSR protocol proposed. Thus, experimental results have shown that the proposed SMPOLSR protocol achieves better performance than existing OLSR, AOMDV, and CA-AOMDV protocols. It has also achieved good results over CA-AOMDV for network packet data protection and produces more energy.

REFERENCES

[1] D. S. Dhenakaran and A. Parvathavarthini, "An overview of routing protocols in mobile ad-hoc network," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, 2013.

[2] P. Periyasamy and E. Karthikeyan, "Survey of current multipath routing protocols for mobile ad hoc networks," *International Journal of Computer Network and Information Security*, vol. 5, p. 68, 2013.

[3] H. Kaur, V. Sahni, and M. Bala, "A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review," *network*, vol. 4, pp. 498-500, 2013.

[4] M. Marimuthu and I. Krishnamurthi, "Enhanced OLSR for defense against DOS attack in ad hoc networks," *journal of communications and networks*, vol. 15, pp. 31-37, 2013.

[5] D. Natarajan and A. P. Rajendran, "AOLSR: hybrid ad hoc routing protocol based on a modified Dijkstra's algorithm," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, p. 90, 2014.

[6] E. S. A. Ganie and M. N. Sharma, "Interference-Aware and Fault Tolerant Multipath Routing Protocols for Mobile Ad Hoc Networks," International Journal of Engineering Science, vol. 2524, 2016.

[7] C. B. Dutta and U. Biswas, "A novel blackhole attack for multipath AODV and its mitigation," in *Recent Advances and Innovations in Engineering (ICRAIE), 2014*, 2014, pp. 1-6.

[8] Vipul Kumar, Musheer Vaqar, "BLACK HOLE Attack: A New Detection Technique", *International Journal of Computer Sciences and Engineering*, Vol.4, Issue.6, pp.63-67, 2016.

[9] K. Somasundaram, "An Effective CBHDAP Protocol for Black Hole Attack Detection in Manet," *Indian Journal of Science and Technology*, vol. 9, 2016.

[10] P. Pavithra, "Averting Techniques of Black-Hole Attack–A Survey," *Indian Journal of Science and Technology*, vol. 9, 2016.

[11] M. S. A. A. Mahmood, D. T. M. Hasan, and M. S. D. S. Ibrahim, "Modified AODV routing protocol to detect the black hole attack in MANET," *International Journal*, vol. 5, 2015.

[12] R. Ahlawat and S. K. Chaturvedi, "A Survey on Black Hole Attacks and Comparative Analysis of Various IDS Schemes in MANET," *International Journal of Computer Applications*, vol. 80, 2013.

[13] Pradeep Kumar Sharma, Shivlal Mewada and Pratiksha Nigam, "Investigation Based Performance of Black and Gray Hole Attack in Mobile Ad-Hoc Network", *International Journal of Scientific Research in Network Security and Communication*, Vol.1, Issue.4, pp.8-11, 2013.

[14] M. K. P. Dubey and E. K. Barua, "A Review-Techniques to Mitigate Black/Gray Hole Attacks in MANET," *Engineering Universe for Scientific Research and Management (EUSRM) Volume*, vol. 6, 2014.

[15] C. She, P. Yi, J. Wang, and H. Yang, "Intrusion Detection for Black Hole and Gray Hole in MANETs," *TIIS*, vol. 7, pp. 1721-1736, 2013.

[16] S. Mandala, M. A. Ngadi, J. M. Sharif, M. S. M. Zahid, and F. Mohamed, "Investigating severity of blackhole attack and its variance in wireless mobile ad hoc networks," *International Journal of Embedded Systems*, vol. 7, pp. 296-305, 2015.

[17] A. Adnane, C. Bidan, and R. T. de Sousa Júnior, "Trust-based security for the OLSR routing protocol," *Computer Communications*, vol. 36, pp. 1159-1171, 2013.

[18] Vinita keer and Syed Imran Ali, "A Survey on Reduction in Energy Consumption by Improved AODV on Mobile Ad Hoc Network", *International Journal of Computer Sciences and Engineering*, Vol.4, Issue.2, pp.54-58, 2016.

[19] Leena Pal, Pradeep Sharma, Netram Kaurav and Shivlal Mewada, "Performance Analysis of Reactive and Proactive Routing Protocols for Mobile Ad-hoc –Networks", *International Journal of Scientific Research in Network Security and Communication*, Vol.1, Issue.5, pp.1-4, 2013

[20] Umesh Kumar Singh, Jalaj Patidar and Kailash Chandra Phuleriya, "On Mechanism to Prevent Cooperative Black Hole Attack in Mobile Ad Hoc Networks", *International Journal of Scientific Research in Computer Science and Engineering*, Vol.3, Issue.1, pp.11-15, 2015.

[21] S. Ali, S. A. Madani, and I. A. Khan, "Routing protocols for mobile sensor networks: A comparative study," *arXiv preprint arXiv:1403.3162*, 2014.

[22] R. K. Gujral, J. Grover, A. Anjali, and S. Rana, "Impact of transmission range and mobility on routing protocols over ad hoc networks," in *Computing Sciences (ICCS), 2012 International Conference on*, 2012, pp. 201-206.

[23] A. S. Otero and M. Atiquzzaman, "Adaptive localized active route maintenance mechanism to improve performance of voIP over ad hoc networks," 2011.

[24] A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq, and T. Saba, "Energy Efficient Multipath Routing Protocol for Mobile Ad-Hoc Network Using the Fitness Function," *IEEE Access*, vol. 5, pp. 10369-10381, 2017.

