CERTIFICATE MECHANISM IMPROVEMENT FOR SECURING OPTIMIZED LINK STATE ROUTING PROTOCOL IN MOBILE AD HOC NETWORKS

[1]ALAA ABDULLAH MAJHOOL, [2] NOR EFFENDY OTHMAN
Center for Software Technology & Management, Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia, Selangor, Malaysia
E-mail: [1]alaa.majhool@yahoo.com , [2] effendy@ukm.edu.my

ABSTRACT

Mobile Ad Hoc Network (MANET) comprises a set of wireless mobile nodes which dynamically generate a temporary network devoid of application of any present network infrastructure and centralized administration. Basically, Optimized Link State Routing (OLSR) is a security problem emanating from attacks. When handling packet forwarding, several types of availability as well as integrity attacks exist, including fabrication, modification, misrouting and dropping whether full or partial. This research utilizes the Secure Optimized Link State Routing (OLSR mechanism which includes certificate authorized nodes (CAs) and RSA algorithm to enhance the security and provide secure routing for OLSR routing protocol, through detection of malicious nodes that perform black hole attack. The proposed protocol is called (SOLS) mechanism. The aim of using the RSA algorithm with certificate authorized nodes (CAs) is to find the secure path from the source to the destination and to detect the black hole attack. We have evaluated the performance of SOLS mechanism by designing simulation using MATLAB. We have compared our mechanism with the performance of protocol OLSR and Baadachi's approach. The comparison was conducted based on the detection ratio, packet delivery ratio, routing overhead, total network load, average delay and source traffic sent & destination traffic received. The SOLS outperformed the Baadachi's approach under wide network performance metrics and settings. The SOLS improved the detection ratio by 4% compared to Baadachi's approach; the implication of this finding is that SOLS can be applied to MANET to detect black hole attack.

Keywords: *Mobile Ad Hoc Network, Ranking Strategy, RSA Algorithm, MATLAB, Optimized Link State Routing, Certificate Authorized Nodes.*

1 INTRODUCTION

MANET security refers to a critical component used to enhance the operation of precise network functions, which are essential for packet routing and forwarding, alongside network management [1]. Therefore, it is essential to include counteractive security mechanisms in such network functions in the early phases of development.

Compared to conventional networks, MANET s offers more accuracy in terms of node performance. In fact, node performance is responsible for the majority of security lapses that occur in networked systems. In a black-hole attack, an attacker targets a specific node whose traffic the attacker wants to intercept. The attacker node advertises itself as having the best path to the targeted node. A flooding-based protocol is used by the attacker to list the request for a route from the initiator. Then, the attacker creates a false reply message to announce the shortest path to the receiver. The attacker's message reaches the initiator first, before the actual node replies. Thus the initiator assumes that the attacker's message is true in indicating the shortest path to the receiver. These results in the creation of a fake route where the attacker is free to exploit the packet sent to the receiver [2].

2 RELATED WORK

Adoni and Tavildar [8] have investigated a strategy on the basis of trust-aware routing; based on the OLSR protocol. The proposed protocol, OLSRM, uses trust-aware routing to enhance the performance of MANETs.OLSRM peformance is assed for single and multi black hole attacks. The performances of MANET utilizing original OLSR and modified OLSRM protocols were compared for a network area of 1000 x1000 square meter.

Baadache and Belmehdi [7] recommended an authenticated end-to-end approach based on acknowledgement to check if the packets are forwarded by intermediate nodes correctly. The function of this approach is to detect the black hole

Table 1 Summary Of Related Work

Researchers	Techniques / Solutions	Introduced New Packets (Yes/No)	Modify OLSR /Routing Tables (Yes/No)	Type of Black- Hole - Attack	Drawbacks
Vani & Rao (2011)	Network-Security protocol is included with the intrusion-detection system	Yes	No	Multiple black holes	Misbehave of multiple black hole attacks
Baadache & Belmehdi (2012)	An approach to verify the correct forwarding of packets by an intermediate node	No	No	Single black hole	Generates a routing overhead slightly more significant than that in the 2-hop ACK approach.
Zougagh & Toumanari (2013)	A novel approach to selecting MPR nodes by additional Coverage	Yes	No	Single & multiple black hole	Less robust routing paths
Baadache & Belmehdi (2014)	An authenticated end-to-end acknowledgment-based approach in order	Yes	No	Single & multiple black hole	No modification and the no replay of messages are required to fully deliver the message to the destination node
Adoni & Tavildar (2015)	A strategy, based on trust-aware routing	Yes	Yes	Single & multiple black hole	High routing overhead This is because OLSRM selects maximum average trust degree path and routes the packets.

conducted normally or co-operatively, the replay of messages and the modifications. Through simulation, performance evaluation and effeciency detection of their approach is shown in both reactive and pro-active routing according to networks in relation to network load and average delay. Besides, there is a comparison between two appraches of watchdog and two-hop ACK based on delivery ratio, additional overhead and detection ratio. approach depicted to have the highest detection ratio and best delivery ratio of packets. However, the generation of routing overhead in watchdog showed a slightly more significant compared to that of the two-hop ACK approach. The limitaion of the approach however, is that it is demanding in terms of resouces.It was forseen that by reducing the the generated communication overhead the approach could be more scalable.

Zougagh et al. [5] proposed a selection of MPRs a new algorithm with the additional coverageThe aim of approach is to ability each node in network to select alternate routs to reach either destination by two hops away. This approach help prevent impact of malicious attacks. The existing algorithm could be easily implemented. the Simulation results show that the proposed approach is effective in reduce black hole attacks. It shows a increases topology acknowledgement and height topology control, that provides many benefits for protocols. the additional knowledge can be provided and build of more strong routing paths, or provide multi paths,To provide security.

Baadache and Belmehdi [3] proposed an approach by employing intermediate node to verification forwarding the correct packets to justification and implementation of the proposed approach ,the author used Merkle tree principle. Through simulation shown the efficiency of approach and they had evaluate its performance in both reactive and proactive routing protocols in a MANETs. likewise, they compared currently approach with the two approach ,the two-hop ACK approach and watchdog approach ; their approach achive the best the highest detection ratio and PDR, but it produce an overhead little more than that in watchdog and the two-hop ACK approaches.

Vani and Rao [4] the authors propose designing a new routing protocol or enhancing the protocol to protect nodes from malicious node and supply a solution for detect security threats. The authors propose a network security protocol that includes an intrusion detection system IDS algorithm. This protocol would observe the network traffic and attempt to investigate activities that fit the patterns of black hole attacks,wormhole attacks, anomalies, failure, channel blocking, and other anomalies behaviour and maintenance in networking . to measure performance of the protocol is measured using end-to-end delay,packet delivery ratio, throughput and routing overhead. Through simulation, the authors have measured the performance of the secure routing protocol. They have used a variety of metrics to measure network parameters under detection of the attack and after detection. The authors have shown the results in terms of node mobility. As the node mobility is increased, the routing overhead increases, and there is little delay as compared to after removal of a threat. Packet delivery ratio and throughput increase after elimination of the attacks.

3 RESEARCH METHODOLOGY

This section discusses about the proposed research methodology taken to achieve the goal of the study. The most popular method of experimentation in terms of network is the simulation. Further, it provides description of the proposed SOLS mechanism and OLSR protocol. It also discusses the implementation that related to the simulation model and the component of the performance metrics that is used to analyse the simulation result. A detailed explanation of working SOLS and finally concluded with conclusion. Figure 1 shows the method .

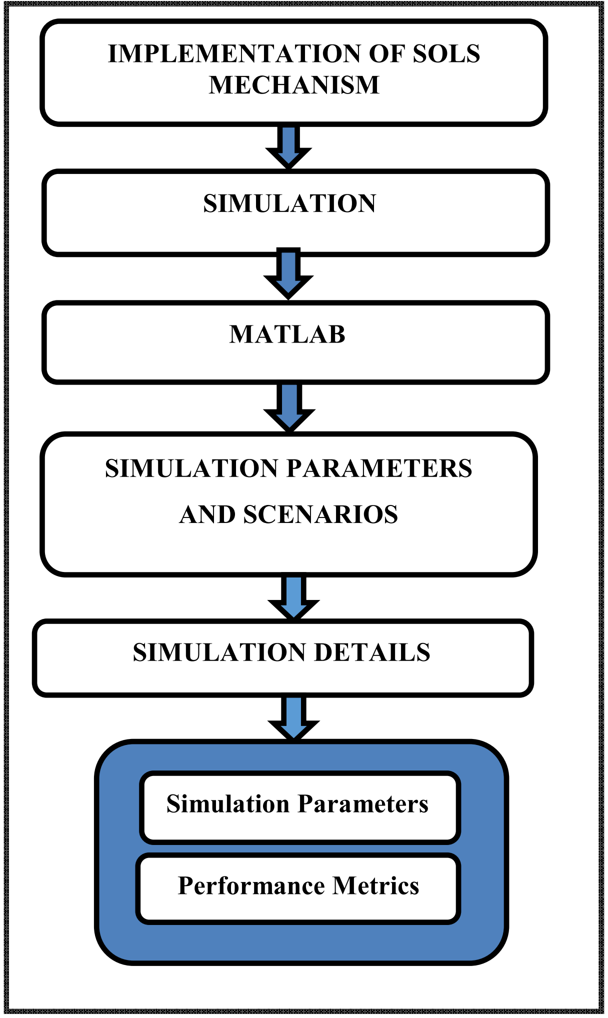


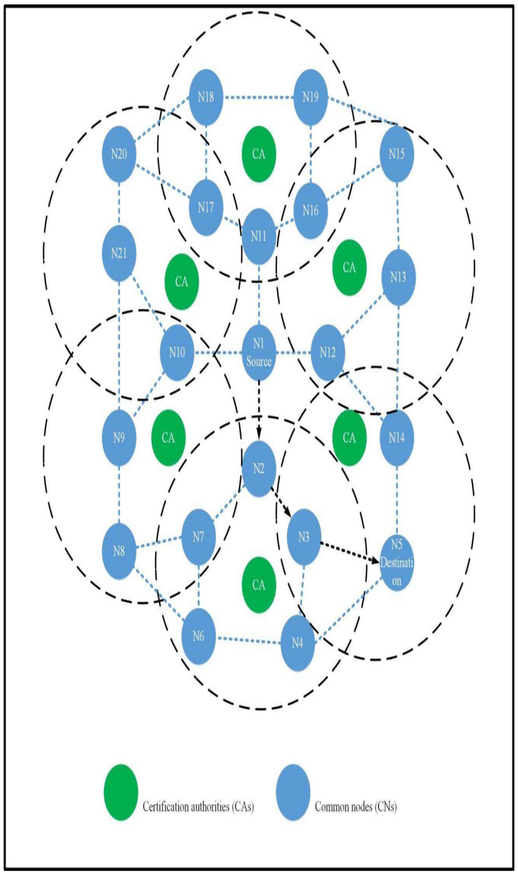
Figure1 Research Method Stage

3.1 Implementation of SOLS Mechanism

The recommended Secure OLSR Protocol (SOLS) is aimed at providing a solution to the security threats. Such solutions comprise of data confidentiality, message and packet integrity, alongside end-to-end authentication is enhanced using a digital signature. Data confidentiality is offered alongside the encryption of the symmetric and asymmetric.

Each communicating node in SOLS requires two pairs of private and public keys cryptography to secure the routing protocol. For instance, node X has verify key, VKX, and sign key, SKX, Likewise, the encryption and decryption keys for Node X are EKX and DKX whereas VKX and EKX are public keys [6].

It is assumed that SOLS utilises the Public Key certificates for distribution as well as management of keys. We employing the RSA algorithm to introduce a new Certificate Authority (CA) mechanism for supervising and managing MANET nodes .For RSA-CA mechanism, SOLS capitalises on the availability of reliable certification servers on the network, known as RSA-CAs and communicating nodes called CNs (common nodes). The RSA-CAs for certification authorities are recognized by all authentic common nodes. Keys are created as a priority and interchanged via a current (and out-of-band) interaction involving the RSA-CA alongside each CN. Prior to joining the network, each node acquires certification from its adjacent RSA-CA. Each node acquires a single certificate following secure authentication of its identity alongside the RSA-CA. Methods exist for secured authentications onto a certificate server, thus such an aspect is at the developers discretion. The certificate of common node X is acquired from the nearest RSA-CA as follows:



RSA-CAs → X: certx= [IPX, VKx, EKx, t, e] | signRSA-CA,

where, signRSA-CA = [IPX, VKx, EKx, t, e] SKRSA-CA.

Node X holds the IP certificate along with VKX and EKX to verify the signature added by X and to encrypt packets to deliver to X, respectively. Additionally, the certificate has a timestamp't' that indicates the time the certificate was produced, and the time of certificate expiry 'e'. The entire information is signed with $_{CA}$ signature for RSA-CA. The node should maintain new certificates together with their nearest RSA-CA. After a node acquires the certificate, its functioning within the network becomes secure.

Figure 1 shows SOLS, whereby N1 represents the source and N5 represents the network destination. Node N1 proactively calculates the routes for all nodes, and N5 stores such data within the SOLS routing table. In this operation, every node in its routing network occasionally advertises the link-state packet (LSP). For instance, the LSP is being advertised by Node ***N1*** in the network as follows:

N1→ brdcast : [LSP, IPN1, certN1, TTL, SNo, neighbour[n], link_metric[n]] | signN1,

where, signN1 = [LSP, IPN1, certN1, TTL, SNo, neighbour[n], link_metric[n]] S.

The packet contains the IP address and certificate for N1, the packet type identifier LSP, sequence number (SNo) of the packet and a time-to-live (TTL) value, the list for ***N1***'s neighbours, alongside the link processes, all carrying the N1 signature sign for ***N1***. The function of the TTL field entails controlling the packet scope, which is initialized onto â-1 hops by ***N1***. The series number is utilised for tracking the history of the link state for the source node N1. After acquiring the packet, the value of TTL is reduced, and if the value exceeds zero, the LSP is retransmitted. When an N1 neighbour acquires the LSP, it determines the packet validity using VKN1 that is extracted from A's certificate within the LSP. This is followed by the neighbour adding the LSP information onto the link-state table, reducing the TTL field value. Afterwards, the LSP is forwarded, if the TTL field value exceeds zero. When the TTL field value is zero, the LSP is discarded. Because each node in network acquires the same LSP, all nodes create a similar link-state table that comprises the fields illustrated below:

<Source-Address, neighbour ID, insert time, route metrics>.

After the link-state table is produced, the nodes compute the route towards all nodes in the network through their link-state table. This data is preserved within the SOLS routing table.

Typically, a SOLS routing table, retained by the node, has various fields that include <Dest-Address, Routes, Route metrics>. Additionally, each node in the network has these elements [6] After the calculation of the proactive route, Node N1 takes the following measures for routing of the data packet onto N5.

Step 1: ***N1*** seeks the route towards ***N5*** within the SOLS routing table and ascertains that it follows the ***N1-N2-N3-N5*** sequence.
Step 2: N1 sends packet of session Key Request (SKREQ) to N5 on the same route and requests the KN1N5 (session key) between ***N1*** and ***N5***:

N1→ N5: [SKREQ, IPN5, certN1] | signN1,
Where, signN1 = [SKREQ, IPN5, certN1] SKN1.

The Session Key Request packet contains IP address of N5, SKREP (packet type identifier) as well as A’s certificate, where all are marked with the signature of N1 utilizing SKN1.After acquiring this request, N5 ascertains the signature with VKN1, obtained from N1 certificate. It then develops the session key KN1N5. The key is then encrypted using EKN1, and sent to N1 as a Session Key Reply Packet (SKREP) using the reversed route ***N5-N3-N2-N1***:

N5→ N1: [SKREP, IPN1, certN5, {KN1N5} EKN1] | signN5,
where, signN5 = [SKREP, IPN1, certN5, {KN1N5}EKN1] SKN5.

This packet comprises N5 certificate, IP address for N1 and SKREP(packet-type identifier), alongside the session key KN1N5 encrypted with EKN1, all carrying N5 signature sign for N5, using SKN5. After acquiring the SKREP, N1 ascertains it using the VKN5, confirming the packet validity, and decrypting it using DK*N1* prior to extraction of the session key KN1N5.When N1 acquires the session key, it begins encrypting the data packet using K*N1N5* and transmits it towards ***N5*** using the same pathway (***N1-N2-N3-N5***). All additional communication involving N1 and N5 occurs in the same way using the same session key [6].

4 EXPERIMENT AND RESULT

This section consists of explains the mechanism of SOLS which includes certificate authorized nodes , RSA algorithm and how it work in a MANETs To provide a safe working environment and detection malicious nodes as black hole attack. We designed simulation using MATLAB to simulate the network because it is necessary to test the theoretical guide mentioned and analysis of the results generated from the simulation test.

4.1 Performance Metrics

The main purpose of the simulation protocol is to evaluate the performance of the protocols, so it is necessary to use performance metrics to evaluate the performance of the Protocol or the comparison between several protocols, represent performance measures quantitative evaluation, 5 metrics were used to evaluate the performance of the network is one of the important metrics under the effect of the black hole attack and a review of the impact of the attack on the performance of the network and through these measures we can evaluate the performance of the network, Which consists of several performance metrics, which will review them below:

4.1.1 Detection Ratio

The traffic that is sent source node indicates the number of packets per second transmitted by the sender node. The traffic that is received by the receiver node (packets/s): shows the number of packets per second which is received by the receiver node. Black hole attack is aimed at preventing packets from reaching the destination. Thus, this study has measured traffic sent source with traffic received destination metric which consider important for detection ratio.

4.1.2 Packet-delivery Ratio

The packet-delivery ratio is the ratio of data packets delivered to the destination to those generated at the source. . This metric presents how a protocol successfully delivers packets from the source to the destination. A high packet delivery ratio indicates good results, which represent the completeness and correctness of the routing protocol. It is calculated by dividing the number of packets the destination node received by the number of packets originating at the source.

$$Packet\ delivery\ ratio = \frac{\sum packets\ received\ by\ destination}{\sum packets\ sent\ by\ sources} * 100$$

4.1.3 Routing Overhead

The routing overhead refer to the ratio of total number of data packets which used in routing to the total number of routing packets delivered to the destination.

$$Routing\ overhead(\%) = \frac{No\ of\ routing\ packets}{No\ of\ routing\ packets + No\ of\ datapackets\ sent} * 100$$

4.1.4 Network Load

The network load refer to the traffic quantity, in (bits/sec) for the whole network, the increase in network load is effect on network efficacy. So, whenever network load less Lead to increase in network efficiency, for measure and evaluate the network performance, we should measure the network load metric.

4.1.5 Average End-to-end Delay

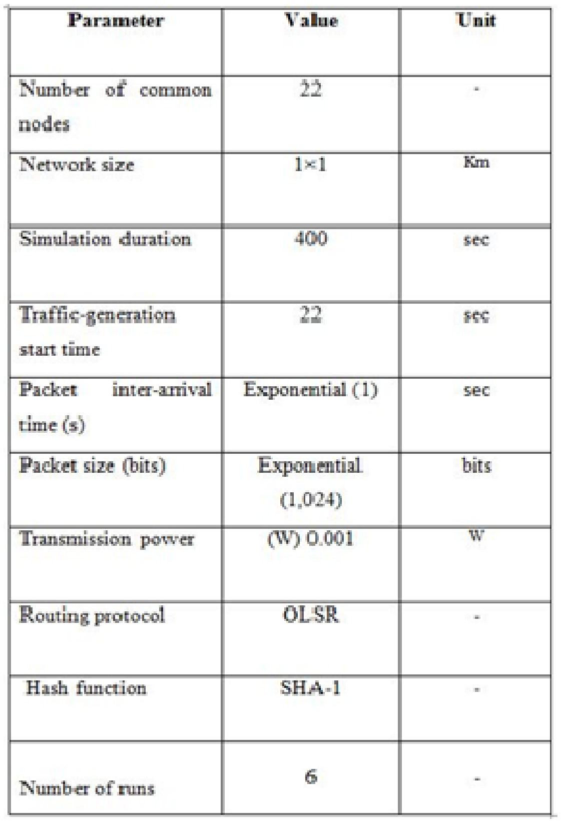
The average end-to-end delay refers to the time it takes for the package sent from the source to the destination successfully, including delays resulting from buffering or delays associated with path finding, which affect the average end-to-end delay. Naturally, the network can be more efficient when the end-to-end delay is small. Hence, we measured the end-to-end delay to evaluate the performance of network. The average end to end Delay is calculated as follows:

$$Average\ End - to - End\ Delay = \frac{\sum_{i-1}^{n}(R_i - S_i)}{n}$$

4.2 Simulation Parameters and Scenarios

In our senario, we measured the detection ratio of SOLS and evaluadted it performance. Simulation parameters are mentioned in Table 3.1. We used 22 nodes isConstant Bit Rate (CBR) and simulation time is 400 seconds for all simulation. Also there are other parameters used in scenario to verify and investigate our mechanism performance such as packet size (bits) exponential (1024), packet inter-arrival time (s) exponential (1), traffic generation start time 20 s, transmit power with 1x1 km simulation area. The traffic (W) 0.001 and random way point mobility model. The network topology could be changing rapidly and randomly unannounced, due to the randomly movement of the nodes. We use the parameters to simulate a network that represents a real scenario. The parameters are varied to investigate their effect on the performance of SOLS mechanism. To validate our result, we must applied the parameters values, metrics and scenario for previous study to compare and validate our result according to previous study such a Baadachi approach(Baadache, A. & Belmehdi, A. 2014) to compare with him.

Table 2 Simulation parameters



Parameter	Value	Unit
Number of common nodes	22	-
Network size	1×1	Km
Simulation duration	400	sec
Traffic-generation start time	22	sec
Packet inter-arrival time (s)	Exponential (1)	sec
Packet size (bits)	Exponential (1,024)	bits
Transmission power	(W) 0.001	W
Routing protocol	OLSR	-
Hash function	SHA-1	-
Number of runs	6	-

5 SIMULATION RESULTS AND DISCUSSIONS

After the simulations were completed for scenario, the evaluation of the performance analysis was conducted using average end-to-end delay, control overhead, and packet delivery ratio ,detection ratio , network load and source traffic sent & destination traffic received evaluation metrics. To indicate the effectiveness of routing protocol OLSR routing protocol using SOLAR mechanism which contain RSA-CA, Conducted a simulation study using different simulation time, the simulation time were 100, 200, 300, and 400 sec. Number of Runs 6 time for each metric one time.

5.1.1 Traffic sent source with traffic received destination

Figure 3 shows the traffic sent source with traffic received destination for OLSR, Baadachi Approach with attack, OLSR with attack and SOLS with attack with the increasing simulation time. Just three test cases showed an increased traffic sent source with traffic received destination when the simulation time in the network is 100, 200, 300 and 400 sec, SOLS with attack increased from 0.32 to 0.37 kbps, Baadachi Approach with attack increased from 0.295 to 0.343 kbps, OLSR without attack increase from 0.326 to 0.377 kbps and case OLSR with attack keep same results However, OLSR without attack has high Traffic sent source with traffic received destination than Baadachi Approach with attack ,SOLS with attack and OLSR with attack. Black hole attack is aimed at preventing packets from reaching the destination. Thus, this study has measured traffic sent source & traffic received destination metric. The traffic that is sent by source node indicates the number of packets per second transmitted by the sender node.

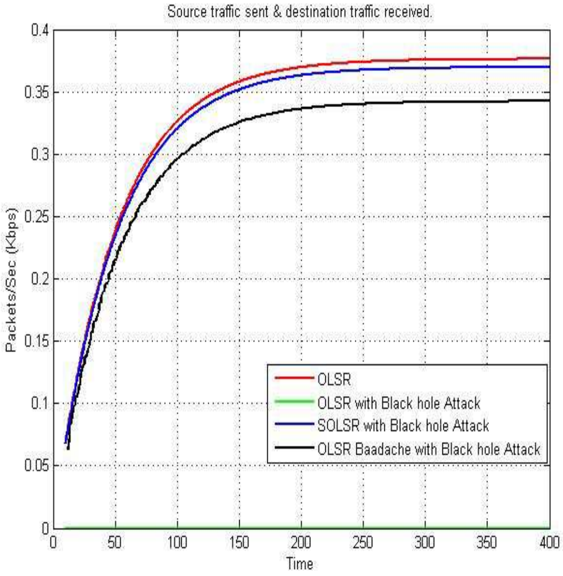


Figure 3 Traffic Sent Source With Traffic Received destination

The traffic that is received by the receiver node (packets/s): shows the number of packets per second which is received by the receiver node. OLSR without attack has best source traffic

Because Baadachi Approach Collects extra routing overhead that is resulted by the control information (the hash of message and the random value) accompanying with exchanged

sent & destination traffic received, in this case we see the traffic received from the destination node the same traffic sent from the source node. The reason is the absence of black hole attack, so the protocol is functioning normally, case SOLS with attack has the lowest rate than OLSR without attack because black hole attack attacking the SOLS so naturally there is a dropping of packets in case of attack.

5.1.2 Communication Overhead

Figure 4 shows the routing overhead for Baadachi Approach with attack and SOLS with attack. With the increasing simulation time, both of test cases showed an increased routing overhead when the simulation time in the network. When the simulation time are 100,200,300 and 400 sec, SOLS with attack increased from 2696 to 2792 bits/sec and Baadachi Approach with attack increased from 3200 to 3512 bits/sec. However, Baadachi Approach with attack has high routing overhead than SOLS. Results clearly indicate that SOLS has the best in terms of routing overhead compared with other routing protocols performance. SOLS got 23% compared to Baadachi Approach. The reason for achieve our mechanism less communication overhead,

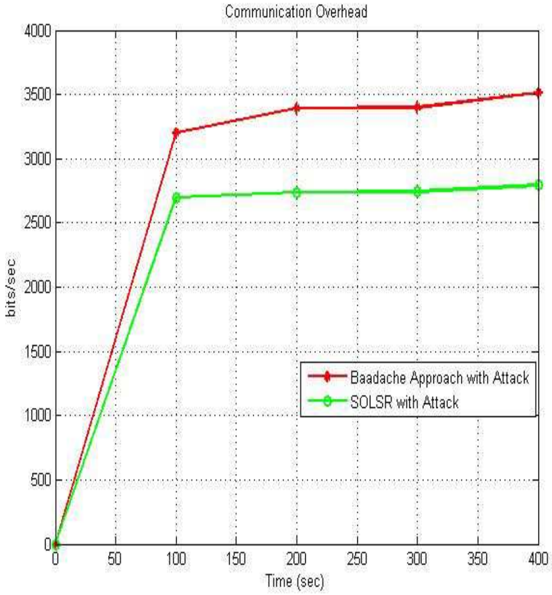


Figure 4 Communication Overhead

acknowledgment between nodes and the messages sent. It indicates increased communication overhead due to increased acknowledgments during the process of routing in the network.

5.1.3 Average Delay

Figure 5 shows the differences of the average end-to-end delay for OLSR, Baadachi Approach with attack and SOLS with attack. When the simulation time increases, the average delay increases. When the simulation time 100,200,300 and 400 sec, OLSR decreased from 1.822 to 0.487 m/sec, Baadachi Approach decreased from 2.016 to 0.103 m/sec and SOLS decreased from 1.04 to 0.106 m/sec. However, SOLS has less average end-to-end delay than both OLSR and Baadachi Approach. Results clearly indicate that SOLS has the best in terms of end-to-end delay compared with other routing protocols performance. SOLS got 60% and 87% compared to Baadachi Approach and OLSR, respectively.

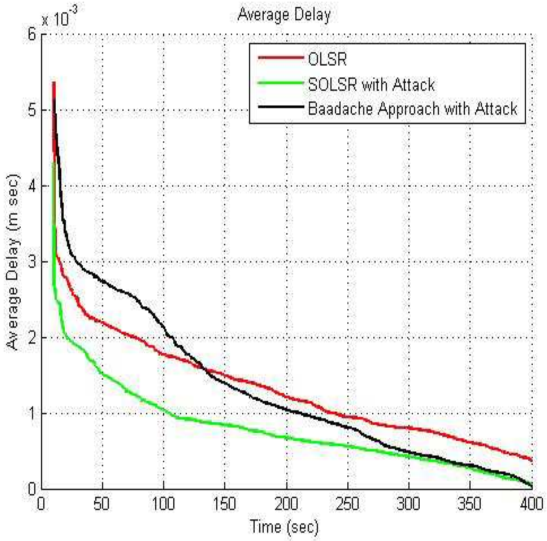


Figure 5 Average Delay

Reason for the delay in Baadachi approach, the source node needs time to check every of acknowledgments received and the discovery of a new route to reach the destination node, SOLS got a lower percentage of delays due has a certificates authorized nodes and exchange certificate authorized between network nodes before entering the network, additionally source node proactively calculates the routes for all nodes, and stores such data within the SOLS routing table. In this operation, every node in its routing network occasionally advertises the link-state packet (LSP),so it is not necessary to change the path through mentoring, thereby reducing percentage of the delay.

5.1.4 Total Network Load

Figure 6 shows the Total Network Load for Baadachi Approach with attack, OLSR and SOLS with attack. With the increasing simulation time, all three test cases showed an increased Total Network Load when the simulation time in the network. When the simulation time is 100,200,300 and 400 sec, SOLS with attack increased from 64 to 370 kbps, OLSR increased from 145 to 277 kbps and Baadachi Approach with attack increased from 64 to 343 kbps. However, SOLS with attack has high Total Network Load than Baadachi Approach with attack. Results clearly indicate that SOLS was not the best in terms of Total Network Load compared with other routing protocols performance. This increase in network load attributed the increase to our solution because source proactively calculates the routes for all nodes; destination stores such data within the SOLS routing table. This operation is called "proactive route computation," whereby every node in its routing network occasionally advertises the LSP (link-state packet). All this represents.

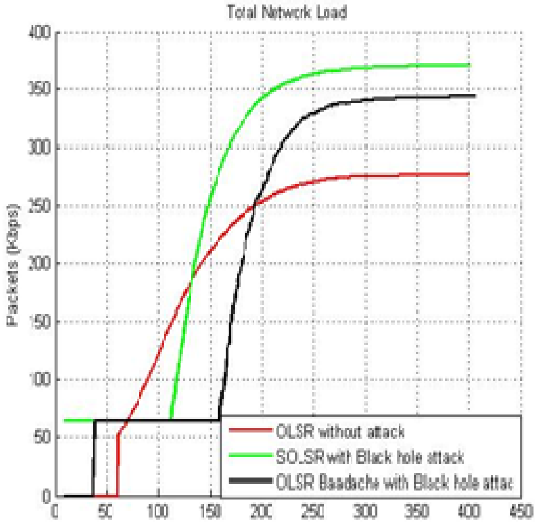


Figure 6 Total Network Load

5.1.5 Packet Delivery Ratio

Figure 7 shows the PDR for Baadachi Approach with attack and SOLS with attack. With the increasing simulation time, both of test cases showed an increased Packet Delivery Ratio when the simulation time in the network. When the simulation time are 100,200,300 and 400 sec, SOLS with attack increased from 89.83 to 95.12(%) and Baadachi Approach with attack increased from

82.32 to 94.18 (%). However, SOLS with attack has high PDR than Baadachi Approach with attack. Results clearly indicate that SOLS has the best in terms of PDR compared with other routing protocols performance. SOLSgot 4.43% compared to Baadachi Approach. The reason is the features of SOLAR mechanism that means detecting malicious nodes and thus avoided, be used as a reliable path for the transfer of packets to the destination and thus ensures the delivery of packets to the destination and less dropping.

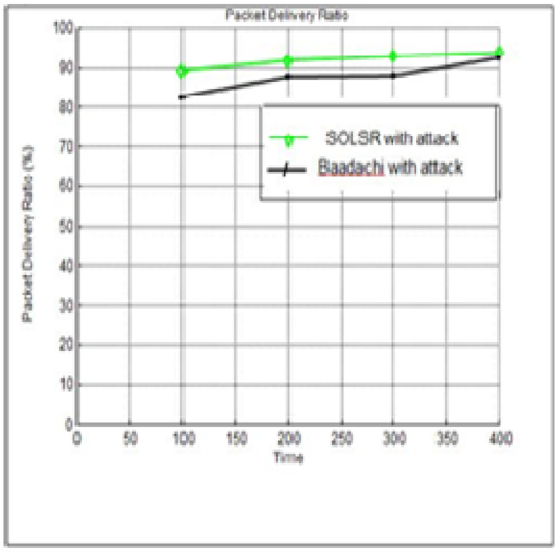


Figure 7 Packet Delivery Ratio

5.1.6 Detection Ratio

Figure 8 shows the differences of the average Detection Ratio for Baadachi Approach with attack and SOLS with attack .when the simulation time increases, the Detection Ratio increases. When the simulation time 100,200,300 and 400 sec, Baadachi Approach increased from78.88 to 81.94(%) and SOLS with attack increased from 81.65 to 85.96 (%) However, SOLS has high Detection Ratio than Baadachi Approach. Results clearly indicate that SOLS has the best in terms of Detection Ratio compared with other routing protocols performance. SOLS got 4% compared to Baadachi Approach. The reason our mechanism achieve high detection ratio than Baadachi approach which provides end-to-end authenticated ACK-based approach that guarantees that the correctness of routing packets through intermediate. It should be noted that to send the message properly to the destination node, no change or repetition of the message is needed. And our mechanism involve RSA algorithm and CA nodes these ensure a data confidentiality, message and packet integrity, alongside end-to-end authentication is enhanced using a encrypt, decrypt, signing and verifying.

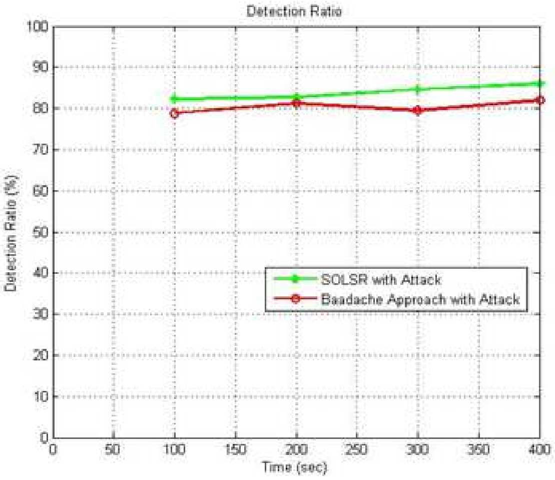


Figure 8 Detection Ratio

5.2 Result Discussions and Validation

To validate our result, we must applied the parameters values, metrics and scenario for previous study to compare and validate our result according to previous study as (Baadache, A. &Belmehdi, A. 2014) to compare with him. We have six metrics for compare with Baadachi approach.

For the comparison the traffic sent source with traffic received destination between SOLS with attack and Baadachi Approach with attack with the increasing simulation time, SOLS test case showed an increased traffic sent source with traffic received destination better than Baadachi Approach when the simulation time in the network is 100, 200, 300 and 400 sec, SOLS with attack increased from 0.32 to 0.37 kbps, Baadachi Approach with attack increased from 0.295 to 0.343 kbps, SOLS got 7.75% average compared to Baadachi Approach.

For the comparison the total network load between SOLS with attack and Baadachi Approach with attack, with the increasing simulation time, both of test cases showed an increased Total Network Load but Baadachi Approach achieve less network load than SOLS, when the simulation time is 100,200,300 and 400 sec, SOLS with attack increased from 64 to 370 kbps and Baadachi Approach with attack increased from 64 to 343 kbps, Baadachi Approach got best result than SOLS, Baadachi Approach got 9.38% average compare SOLS.

For the comparison the routing overhead between Baadachi Approach with attack and SOLS with attack, with the increasing simulation time, both of test cases showed an increased routing overhead when the simulation time in the network but SOLS a chive less routing overhead than Baadachi Approach, when the simulation time are 100,200,300 and 400 sec, SOLS with attack increased from 2696 to 2792 bits/sec and Baadachi Approach with attack increased from 3200 to 3512 bits/sec. However, SOLS achieve best result than Baadachi Approach. .SOLS got 20.67% average compared to Baadachi Approach.

For the comparison the packet delivery ratio between Baadachi Approach with attack and SOLS with attack, with the increasing simulation time, both of test cases showed an increased Packet Delivery Ratio when the simulation time in the network. When the simulation time are 100,200,300 and 400 sec, SOLS with attack increased from 89.83 to 95.12(%) and Baadachi Approach with attack increased from 82.32 to 94.18 (%). However, SOLS with attack has high PDR than Baadachi Approach with attack. SOLS got 4.42% average compared to Baadachi Approach.

For the comparison the average end-to-end delay between Baadachi Approach with attack and SOLS with attack. When the simulation time increases, the average delay decreases for both case. When the simulation time 100,200,300 and 400 sec, Baadachi Approach decreased from 2.016 to 0.103 m/sec and SOLS decreased from 1.04 to 0.106 m/sec. However, SOLS has less average end-to-end delay than Baadachi Approach SOLS got 28.86 % average compared to Baadachi Approach.

For the comparison the detection ratio between Baadachi Approach with attack and SOLS with attack .when the simulation time increases, the Detection Ratio increases for both case, when the simulation time 100,200,300 and 400 sec, Baadachi Approach increased from78.88 to 81.94(%) and SOLS with attack increased from 81.65 to 85.96 (%) However, SOLS has high Detection Ratio than Baadachi Approach. Results clearly indicate that SOLS has the best in terms of Detection Ratio compared with other routing protocols performance. SOLS got 4% compared to Baadachi Approach.

6. Conclusion

In our study, we evaluated three routing protocols. OLSR, SOLS and Baadachi Approach .we are evaluated the performance of these protocols through Scenario. provides for the effect of time simulation under black hole attack, using metrics such as end to end delay, network load ,communication overhead, packet delivery ratio, detection ratio and Traffic sent source with traffic received destination, the reason to measure this metric is that the black hole attack prevents arrival of the source packets to the destination. Finally, the results of simulation indicate that SOLS mechanism achieved the best results in most of the tests compared with OLSR and Baadachi Approach. The successful use of certificate authorized nodes (CAs) and RSA algorithm in many MANET applications motivated this research to adapt the certificate authorized nodes (CAs) and RSA algorithm to improve the security OLSR routing protocol. The present study proposed a Detection malicious nodes that affect the security network, providing security Routing for OLSR, Mentioned in Introduction of certificate authorized nodes (CAs) and RSA algorithm .The results of the simulation for SOLS significant improvements within the network parameter settings, such as time simulation.

REFRENCES:

[1] Alnaghes, M. S. & Gebali, F. 2015. A Survey on Some Currently Existing Intrusion Detection Systems for Mobile Ad Hoc Networks. *The Second International Conference on Electrical and Electronics Engineering, Clean Energy and Green Computing (EEECEGC2015)*, hlm. 12.

[2] Kaur, S., Bansal, K. & Bansal, S. 2013. Performance Analysis of AODV, DSR and OLSR Routing Techniques for Ad hoc Mobile Networks. *International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)* 3(5): 195-200.

[3] Baadache, A. & Belmehdi, A. 2014. Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks. *Computer Networks* 73: 173-184.

[4] Vani, A. & Rao, D. S. 2011. Providing of Secure Routing against Attacks in MANETs. *International Journal of Computer Applications (0975–8887) Volume*:

[5] Zougagh, H., Toumanari, A., Latif, R. & Idboufker, N. 2013. A novel security approach for struggling black hole attack in optimised link state routing protocol. *International Journal of Sensor Networks* 18(1-2): 101-110.

[6] Pani, N. K. & Mishra, S. 2014. Secure Hybrid Routing for MANET Resilient to Internal and External Attacks. *ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol I*, hlm. 449-458.

[7] Baadache, A. & Belmehdi, A. 2012. Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks. *Journal of Network and Computer Applications* 35(3): 1130-1139.

[8] Adoni, K. A., & Tavildar, A. S. 2015. Trust aware routing framework for OLSR protocol to enhance performance of Mobile Ad-Hoc Networks. *In Pervasive Computing (ICPC), 2015 International Conference on (pp. 1-7). IEEE.*