ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

NISD: A Node ID Based Secure Detection and Isolation System for OLSR Routing Protocol in MANETs

[1]Dhanalakshmi Natarajan and [2]Alli P Rajendran

[1]*Research Scholar, Department of Information Technology, NPR College of Engineering & Technology, Dindigul, Tamil Nadu, India.*
[2]*Professor & Head, Department of CSE, Velammal College of Engineering & Technology, Madurai, Tamil Nadu. India*.

ARTICLE INFO

Article history:
Received 12 March 2015
Accepted 28 April 2015
Available online 5 May 2015

Keywords:
Dijkstra Algorithm, Intrusion Detection and Isolation, Malicious Nodes, Mobile adhoc networks (MANET), Multi Point Relays (MPR), Node ID Based Secure Detection (NISD), Optimized Link State Routing (OLSR), TC messages and Time-To-Live (TTL).

ABSTRACT

Background: NISD: A Node ID Based Secure Detection and Isolation System for OLSR Routing Protocol in MANETs. **Objective:** The Optimized Link State Routing (OLSR) protocol is a recognized route discovery protocol used for Mobile Adhoc Networks (MANET). It enhances the link state information through the network with the proposed selection of Multi Point Relays (MPRs). Moreover, Intrusion Detection and Isolation in MANET are essential to formulate a strong security mechanism. Hence, it is mandatory to understand about how the malicious nodes are attacking the network. To overcome the security issues, this paper focuses on Intrusion Detection and Isolation (IDI) System in the AOLSR protocol to enable the trusted source to destination communication. The modified Dijkstra Algorithm is used to obtain the multiple paths. A novel Node ID Based Secure Detection (NISD) Method is proposed to overcome the security issues. The proposed NISD accurately identifies and isolates the malicious nodes in the routing path and establishes the trusted link from source to destination. The experimental results of the proposed NISD method is compared with the existing OLSR and Advanced OLSR (AOLSR) protocols. It shows that the proposed NISD system yields better performance than the existing protocols in terms of packet delivery ratio, average end-to-end delay, and average time waiting in queue. **Result and Conclusion:** The Modified Dijkstra Algorithm provides the flexible and scalable multiple disjoint paths between any two nodes of the network. Furthermore, NISD is compared with the existing OLSR and AOLSR protocols. With the presence of malicious nodes, the proposed method results above 80% packet delivery ratio.

© 2015 AENSI Publisher All rights reserved.

ToCite ThisArticle: DhanalakshmiNatarajan and Alli P Rajendran., NISD: A Node ID Based Secure Detection and Isolation System for OLSR Routing Protocol in MANETs. ***Aust. J. Basic & Appl. Sci.,*** *9(11): 149-159, 2015*

INTRODUCTION

Mobile Adhoc Networks (MANET) is a collection of mobile nodes or computers that together forward the data packets to each other in a limited transmission range of each other's mobile network interface. It is an infrastructure less network, implies that the network without the usual routing infrastructure such as routing backbones and fixed routers. A routing protocol finds the path in the network among nodes, which permits a data to be forwarded through other network nodes to its destination.Many routing protocols have been implemented (Garg,N.,*et al*., 2012). It can be categorized in accordance with various criteria. The major classification nature is the type of route discovery. The two categories of the routing protocols are proactive routing protocols and reactive routing protocols. In reactive protocols, the routing request is sent on-demand basis; if a node wants to make a communication with other node, it broadcasts a Route Request (RR) packet and expects a response packet from the corresponding destination node. Some examples of the reactive protocols are *Dynamic Source Routing* (DSR) (Gawande, A., 2013) and *Adhoc On-demand Distance Vector Routing* (AODV) (Hinds, A., *et al*., 2012). Conversely, proactive routing protocols are update their routing information in order to have a permanent view of the network topology. Example of proactive routing protocol is *Optimized Link State Routing* (OLSR) protocol (ArifaAzeez, A.A., *et al*., 2011).

Another criteria for the classification of adhoc routing protocols is the total number of routes estimated between the source and destination. The two categories are single path routing protocols and multipath routing protocols. MANET is more prone to link and node failures due to the node expiration or node mobility. The path used for routing may break down for various reasons. In order to improve the routing resilience against the link or node

Corresponding Author: DhanalakshmiNatarajan, Research Scholar, Department of Information Technology, NPR College of Engineering & Technology, Dindigul, Tamil Nadu, India.

failures. One solution for this problem is to route the packet through multiple disjoint paths simultaneously. Due to the dynamic, infrastructure less nature and openness of wireless links, the MANET routing protocols faces severe security problems. Moreover, any node participating to the routing can easily attack the MANET by distracting any transmission or the node compromising the routing tables or other nodes. The multipath routing approach attempts to mainly focus the problems of mobility, scalability and link stability of the network. But, it lacks to provide the secure routing facility in multipath fashion.According to the multipath routing protocols, there are 3 key challenges to be addressed. 1) Discovery of multiple disjoint routes with common nodes or links, 2) multiple paths can be simultaneously used for parallel data transmission and 3) load distribution.

In the proposed method, the security issues related to the discovery of routes or selection of paths in multipath OLSR routing protocol is addressed. There are several types of attacks are possible on OLSR protocol. In order to improve the resilience against security issues, a node may formulate a disjoint paths. The flooding of link state information has also been tampered through misbehaving nodes on the network. The multipath routing mechanisms with the selection of MPRs are susceptible to these kind of attacks. Mostly, the attacks have impact in *topology discovery* stage or *route computation* stage.In[5-8], the multipath extension to OLSR (MP-OLSR) is discussed. It is a hybrid routing protocol with multiple defined coding for data transfer. The optimal routes are identified based on the Dijkstra algorithm in terms of hops. MP-OLSR does not consider the security measures. Moreover, the calculated routes are not essentially disjoint. The proposed system includes the Intrusion Detection System (IDS) to overcome the drawbacks of the existing OLSR protocols.IDS can accurately detect the malicious nodes based on the End-to-End communication from the source node to the destination node.

The proposed method uses the OLSR protocol with the modified Dijkstra algorithm to find out the shortest path from the source to destination node. During the MPR selection process, an attacker node disrupts the flooding of topology control information by misbehaving the information. We proposed a novel Node ID Based Secure Detection (NISD) Method to overcome the security issues. Here, the MPR set is selected based on the Node ID and the random number generated based on the key generation concept. The beacon message is distributed periodically to know about the neighboring nodes. It helps to identify the misbehaving nodes by validating the keys. If any misbehaving nodes are identified, then re-authentication process takes place to select the authenticated MPR set for data forwarding. This process gets repeated until the authenticated MPR set is identified. The misbehaving nodes are isolated and blocked based on the Malicious Node Detection Algorithm. The proposed method can able to identify malicious nodes that might occur between the source to destination path.

The remainder of this paper is organized as follows. Section 2 summarizes the existing works related to the security issues and solutions for OLSR protocol. Section 3 describes about the OLSR protocol and its security issues. Section 4 presents the proposed Node ID based Secure Detection (NISD) method. Section 5 describes the performance analysis. And finally, the paper is ended with the conclusion at section 6.

Related Works:

The mobile environment includes a number of security issues that need to considered and addressed. Some of the issues are associated to the physical nature of the mobile nature. Whereas other problems are related to the wired network. This section deals with the works related to the multipath disjoint strategies in OLSR protocol and the security models incorporated into the OLSR protocol. *Zhihaoet al*proposed a multi objective method for proactive routing in MANET. It achieves the following three objectives such as reducing average end to end delay, increasing the network lifetime and maximizing the packet delivery ratio. For each node, the link stability, cost and delay were calculated. The double exponential smoothing was used to predict the queuing delay and energy consumption. A heuristics distribution was used to predict the residual lifetime of the link (Guo, Z., *et al*., 2011).*Jiazi et al* designed a multipath optimized link state routing. The multipath Dijkstra algorithm was used to obtain the multiple paths from source to destination. Route recovery and loop detection have been implemented in the multipath OLSR protocol to improve the Qualityof Service (Yi, J., *et al*., 2011).

*Sun etal*formulated a delay constraint multipath routing protocol. The HELLO message and topology control message were used to analyze the link delay among the nodes and gathers the delay information. Also, the multipath Dijkstra algorithm was used for path selection to reduce the delay path from the source to other nodes. Various node disjoint or link disjoint multipath has been formulated through the route computation after the route was established (Sun, Y., *et al*., 2014).*Gimeret al* proposed an OLSR protocol for MANET routing. The MultiPoint Relays was selected based on the improved flooding mechanism for distributing the link state information. It leads to reduce the size and total number of control traffic messages. Here, Hierarchical OLSR was used to address the scalability and fault tolerance issues (Cervera, G., *et al*., 2013). Some of the OLSR security vulnerabilities are (Zheng, S., *et al*., 2008):

1. Identity spoofing

2. Link spoofing
3. Traffic relay refusal
4. Replay attacks
5. Wormholes.

*Asmaet al*formulated a trust based security for OLSR routing protocol. The trust based analysis was done based on the trust specification language. Here, each node evaluates the behavior of the other nodes (Adnane, A., *et al*., 2013).Another topic of research concerns an intrusion detection. *Abdalla et al* designed a misbehavior nodes detection and isolation mechanisms in OLSR protocol. Intrusion Detection Systems (IDS) were used to detect and isolate the attacker nodes based on End to End (E2E) communication. The relationship between the neighbor nodes decides the other node to eliminate the misbehavior nodes from the routing table. It leads to select the trusted nodes for data forwarding from source to destination (Abdalla, A.M., *et al*., 2011).*Bose et al*introduced an Efficient Secure Routing Protocol (ESRP) based on the trusts computation. The trust value results an integer value to select the administrator node for routing (Bose, D., *et al*., 2012).

*Shaw et al*proposed a spoofing attack identification mechanism in OLSR protocol. Here, the number of possible attacks occurred against the integrity of the OLSR infrastructure was enumerated (Shaw, S., *et al*., 2011). *Cerveraet al* discussed a mitigation of topology control traffic attacks in OLSR. An improved MPR set was selected with additional coverage. Ever node selects the possible k+1 disjoint MPR sets. Alternative paths were formulated to obtain any two hop destinations. The MPR with additional coverage can mitigate the effect of the control traffic attacks (Cervera, G., *et al*., 2010).*Ranaet al*presented a defending mechanism against node misbehavior to discover the secure route in OLSR. The security features were based on the authentication checks on the information. The authentic route confirmation ticket was used to regulate the behavior of nodes. This mechanism was used to prevent the network from internal attacks (Rana, S.and A. Kapil, 2010).*Jan Maarten etal*analyzed the lifetime of the OLSR networks. The MPRs were used for forwarding the control traffic. The maximum forcedness ratio was used as k key parameter of the network to define the lifetime results of the MPR selection heuristics (Verbree, J.-M., *et al*., 2010).*Marimuthuet al*proposed anenhanced OLSR protocol against a Denial of Service (DOS) attack called node isolation attack. Based on the HELLO packets, it can identify that the node was advertising a correct topology information or not. This technique was light weighted because it doesn't include any high computational complexity for network security (Marimuthu, M.and I. Krishnamurthi, 2013).

Another area of research concerns the intrusion detection on the routing protocols. The overall function of an IDS is detecting the misbehavior nodes by analyzing the network traffic (Chowdhary, M., *et al*., 2014). *Ahmed et al* introduced an Intrusion Detection System to identify the misbehavior nodes in OLSR protocol. IDS accurately identifies the misbehavior nodes based on the end to end communication from the source and destination (Abdalla, A.M., *et al*., 2010). Usually, the feedback mechanism was used to secure the OLSR against the link spoofing attacks.*Saroitet al*presented an IDS mechanism to secure the OLSR protocol. This mechanism was based on three ID messages such as Attacker Finder Message (AFM), Attacker Isolation Message (AIM) and Path Validation Message (PVM) (Saroit, I.A.and A. Kotb, 2013).*Lekovaet al*proposed a Reliable OLSR (ROLSR) for detecting and isolating the selfish nodes. The data traffic was regularly monitored on each MPRs. The abnormalities in the traffic patterns on MRPs denotes the selfishness and initiates the topology update step to isolate the malicious nodes (Lekova, A.and M. Adda, 2013).

OLSR Protocol and Security Issues:

OLSR Protocol:

OLSR is the proactive routing protocol, especially formulated for MANET. It periodically exchanges the routing information and select the optimal route when needed. It achieves optimization by determining for each node of the network with a minimal subset of neighbors termed as Multi Point Relays (MPR) that are able to extend all 2-hop neighbors of the node. Basically there are two types of routing packets are used (Yi, J., *et al*., 2011).

1. HELLO packet
2. Topology Control packet.

HELLO packet is broadcasted periodically by each node and it the packet includes the senders identity such as list of neighbor nodes for which the control traffic had been heard, list of neighbor nodes with which bi-directionality had been already confirmed and the list of MPR set of originator node. Mainly, HELLO message is utilized for *neighbor sensing* and the *selection of MPRs*.

TC packets are also periodically broadcasted by MPR nodes. The packet includes the set of the senders MPR selector set. In this protocol, MPR nodes only responsible for TC forwarding. Basically, TC packet can be used for *route calculation*.

Operations of OLSR

The operations of OLSR protocol can be summarized in fig.1. In neighbor sensing, each node broadcast the HELLO packet to its 1 hop neighbors periodically. Then, MPR selection has two types of sets. One is MPR set, it is the selected neighbors of each node from its one hop neighbors. If a node forwards the routing message, then only the nodes in the MPR set can forward the message. Another one is called MPR selector set, where each node manages

the information about the list of neighbor nodes that are selected as MPR.Later, MPR nodes should send the TC packet to formulate the routing table. TC packets are broadcasted in the network and MPRs only permitted to transfer the TC packets.

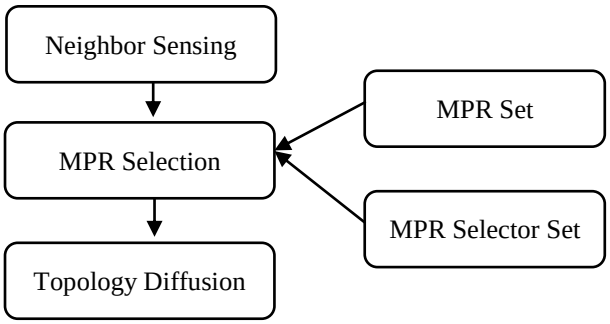

Fig.1: Operations involved in OLSR protocol

Every node in OLSR protocol correctly generates the control traffic and routing. Also, the nodes can correctly relay the routing control traffic on behalf of another nodes.

Security issues of OLSR:

1. There are no security approaches for a trusted node to differentiate a malicious node from the neighbor node, once the attacker includes the MPR node. Then the attacker can establish a black hole attack to drop all the messages or eavesdrop the content and relay it other malicious node. It affects the trusted node performance.
2. An attacker node creates false topology control message for broadcasting. Because, there is no more source authentication, or other nodes accept it and update the global topology information.
3. The AOLSR protocol doesn't protect the routing packets in the adhoc networks. Hence, a malicious node can easily alter the message and it won't be isolated.
4. The AOLSR protocol uses the HELLO packets for neighbor detection, which leads to wormhole attacks.

Security Requirements:

1. It is necessary to provide a mechanism to identify the warm hole attack during the neighbor node detection;
2. It is necessary to import identity authentication before two nodes initiate to start the neighbor relationship. It prevents the malicious nodes becomes a trusted nodes (MPR node);
3. It is necessary to verify the sender routing packets is the one it claims to be;
4. Moreover, it is necessary to check that the arrived routing packet has not changed at the data transmission.

NISD: A Novel Node ID based Secure Detection:

The proposed system incorporates the Intrusion Detection Isolation System into the standard OLSR protocol. The OLSR protocol uses the modifiedDijkstra algorithm to find out the shortest path from the source to destination. The proposed system uses the *Modified Dijkstra Algorithm.* DhanalakshmiNatarajan and Alli P Rajendran, 2014).The proposed method introduces a Node ID based Secure Detection (NISD) algorithm to isolate and block the misbehaving nodes from the communication among nodes.Initially, all the nodes are generating and distribute the key with each other. Based on the NISD algorithm, an authentication validation is checked with the corresponding keys. It is necessary to retrieve an authenticated MPR set to formulate a secure and trusted communication. Here, the MRP selection procedure is continued until the set contains only the authenticated nodes. The multiple paths are identified using the modified Dijkstraalgorithm.The flow of the proposed Intrusion Detection and Isolation System for AOLSR protocol is illustrated in fig.2.

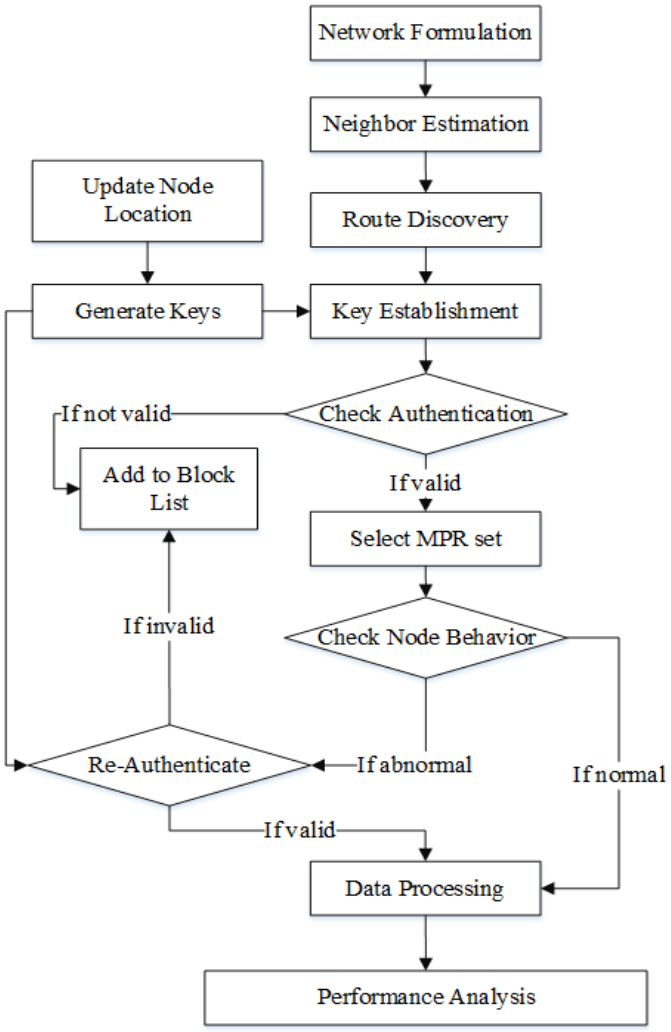

Fig.2: Flow of the proposed NISD

The neighbor nodes are selected based on the following eqns:

$NeighborSelection = E_i^t - ((L_i^t * UE_i) + TE)$(1)

$t_r = \frac{\alpha_i}{\alpha_i+\beta_i}$ (2)

Table 1: List of Notations

Symbols	Descriptions
E_i^t	Energy for ith node
L_i^t	Energy for ith node
UE_i	Unit Energy Consumption
TE	Transmission Energy
t_r	Trust
α_i	Successful communication
β_i	Failure communication.

The path recovery and loop discovery stages are explained in (DhanalakshmiNatarajan and Alli P Rajendran, 2014).

NISD: Intrusion Detection and Isolation System:

In the proposed NISD protocol, there are two level of procedures are proposed to remove the malicious nodes from the data transmission.The security of AOLSR is categorized into three levels.

1. *MPR set* (malicious node may include into the MPR set)
2. *TC message* (malicious node may include the list to forward the TC message)
3. *Hop count* (based upon the hop count value or the Time-To-Live (TTL) measure the malicious node can be detected.

The MPR set includes the malicious nodes, which is shown in fig.3. The header includes the information about the malicious nodes. It will

remove from the routing and add it into the block list. Each intermediate node, which receives the Malicious Identification Message is reply back to *s*. It includes the information regarding the hop count and the next node to *d*.

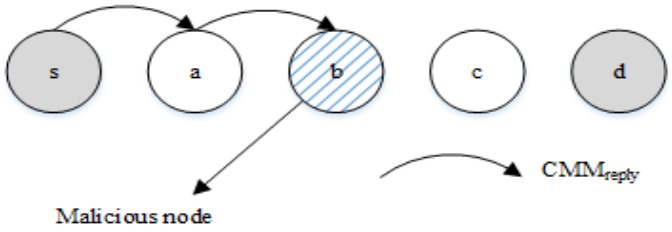

Fig.3: Malicious node drops packet

Here CMM denotes Crosschecking MPR message reply. Node *s* waits for an acknowledgment message from the intermediate nodes for a predefined period of time. In order to remove the malicious nodes from the path, we proposed a NISD algorithm and it is described as follows.

Algorithm 1 Node Id Based Secure Detection

Initial level malicious detection:
Input: S_{ID}, D_{ID}, S_n, S_x, S_y
Output: Malicious Node
Begin

//Key Generation:
For all S_n
$K(S_{ni}) => S_{niId} \oplus S_x \oplus S_y$
Broadcast $K(S_n)$ *to* S_n
End

// Authentication:
If Receive RREQ

// Check Authentication Key:
If $K(S_n)$ *of In-Valid*
Add to block list
Else
Data processing
End if
End if
End

Re-authenticationVerification:
Input: S_{ID}, D_{ID}, S_n, S_x, S_y
Output: Misbehavior Nodes
Begin

// Check Misbehavior Node:
Analysis traffic flow
If traffic flow is high
Check Re-Authentication using updated key
If Updated $K(S_{ni})$ *is invalid*
Add to block list
Else
Data processing
End if
End if
End

Here, the source ID (S_{ID}), destination ID (D_{ID}), source neighbors (S_n), and the position of the source nodes (S_x, S_y) are given as the input. Initially, all the neighbor nodes are generated a key based on the position of the neighbor nodes and the corresponding neighbor node ID. Then, broadcast the key to the neighbor nodes. If the node receives the RREQ, then it is further validate that whether the key is valid or not. If the key is identified as invalid, then the node will be send into the block list. Otherwise, it is used for data processing. After identifying the MRP set, the data packet is forwarded from source to destination. At the time of routing, it is possible to attempt the misbehavior nodes to eavesdrop the information. Hence, a re-authentication procedure gets initiated, which analyzes the traffic flow for the transmission. If the traffic is high, then it is further check for the key information. The invalid key nodes are moved to the block list. Otherwise, the packet is transmitted. This process gets repeated until all the successful path is identified to deliver the packet in a secure environment.

Performance Analysis:

In this section, the experiments are conducted to measure the effectiveness of the proposed Node ID based Secure Detection (NISD) method. The goal of this approach is to increase the chances of calculating the multiple node disjoint routes in OLSR protocol. There are 100 nodes are taken for the result analysis. Moreover, the malicious and misbehaving nodes are not included to perform the attack on the network. The standard OLSR protocol is incorporated with the Intrusion Detection algorithms to provide trusted communication between the source and destination nodes. The proposed NISD system is compared with the existing standard OLSR protocol and the Advanced OLSR protocol (DhanalakshmiNatarajan and Alli P Rajendran, 2014). The effectiveness is validated based on the following metrics: Packet Delivery Ratio, Number of TC messages, End-to-End Delay (E2E), and the average time. Table 2 shows the simulation parameters for the proposed method.

Table 2: Simulation Parameters

Simulation Parameters	Values
Number Of Nodes	100
Network Interface	Channel/Wireless
NS Version	NS-2.34
Packet Size	512 bytes
Interface Queue	DropTail
Interface Queue Length	100000 Bytes
Simulation Area	600 X 600 mSq
Simulation Duration	100 ms
Packet Rate	11 bps
Initial Energy of node	100 J
Transmitting Energy	0.1 J
Receiving Energy	0.1 J

Various multipath routing protocols utilizes the advantages of the proactive properties and the MPR flooding mechanism used in the OLSR protocols. The proposed NISD also uses the advantages with the intrusion detection strategies to result higher packet delivery ratio. Based on the Dijkstra Algorithm, the nodes can easily compute the multipath paths.

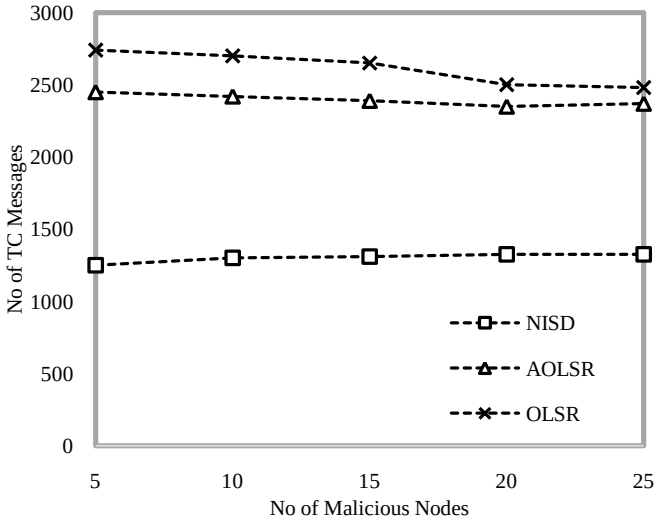

Fig.4: Simulations to compare the proposed NISD with existing OLSR and AOLSR against number of TC messages with number of malicious nodes (up to 25 nodes)

There are 25 malicious nodes are taken to validate the proposed system and the total number of TC messages and the resultant PDR ratio are examined. If the malicious nodes include the intermediate node set from source to destination, then the packet will be lost or the packet includes some wrong information. The NISD can remove the malicious nodes from the MPR set and the entire network. With the interruption of malicious nodes, the proposed system generates lesser TC messages than the existing AOLSR and OLSR protocols. Fig.4 shows the generation of TC messages due to the malicious nodes interruption on the network. The proposed system can withstand better even it includes the misbehaving nodes. Because, the NISD algorithm can detect and isolate the malicious nodes into the block list. Hence, only the authenticated nodes will transmit the packets to the destination nodes. As the TC messages reduces, it automatically decreases the E2E delay and average time.

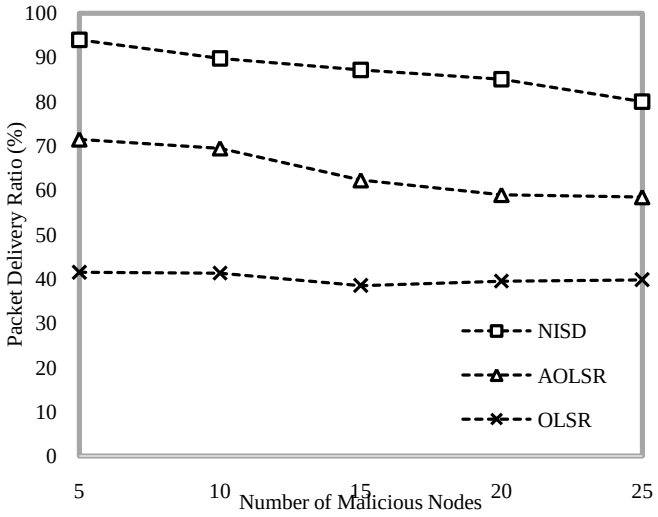

Fig.5: Simulations to compare the proposed NISD with existing OLSR and AOLSR against PDR with number of malicious nodes (up to 25 nodes)

The proposed method only uses the authenticated MPR set to forward the packets. Hence, it is not possible to misuse the packets or any failures may occur. Then, automatically the packet delivery ratio is increased. Fig.5. shows that the proposed NISD results higher packet delivery ratio than the existing OLSR and AOLSR protocols. The packet delivery ratio is examined by varying the node speed upto 10m/s. It also results better results than the existing method which is shown in fig.6.

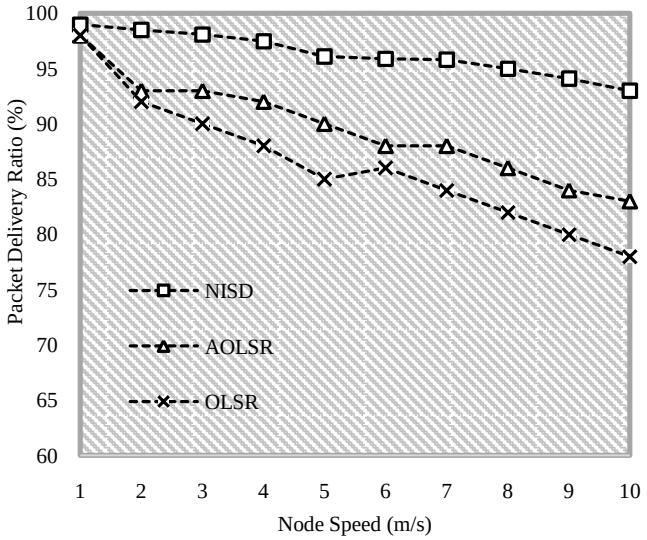

Fig.6: Simulations to compare the proposed NISD with existing OLSR and AOLSR against PDR with varying node speed

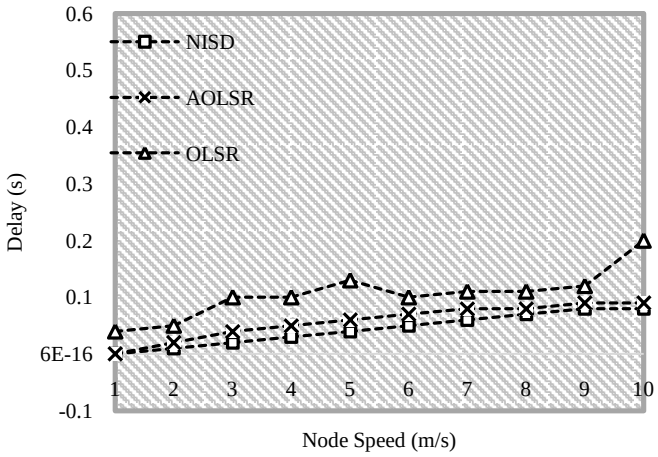

Fig.7: Simulations to compare the proposed NISD with existing OLSR and AOLSR against delay for 1-hop neighbors with varying node speed

Fig.7. shows the simulation result for the time taken to forward the control traffic and data traffic between 1-hop neighbors. The result is compared with the existing protocols to show the efficiency of the proposed NISD protocol. The proposed NISD protocol results lesser 1-hop delay than the existing protocols.

The E2E delay comes for the following two major reasons:

1. The network takes more time to detect and isolate the malicious nodes from the network.
2. Since the malicious node damages the routing path, the process to determine the alternative routing path requires additional time.

For the above two stated reasons, the time to transmit the packet from source to destination takes more time. But, the proposed system effectively detects and isolates the malicious nodes from the routing path. Hence recalculation of routing path is not required for data transmission. It significantly reduces the E2E delay from the source to destination.

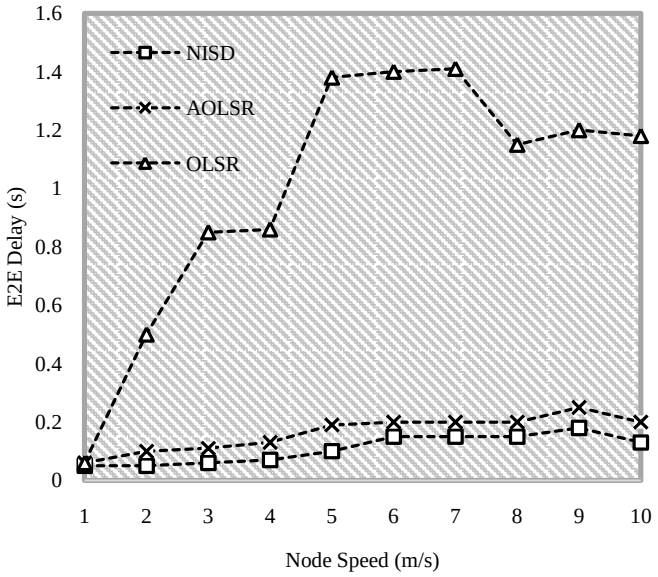

Fig.8: Simulations to compare the proposed NISD with existing OLSR and AOLSR against E2E delay with varying node speed

Fig.8 depicts the variation of the average E2E delay with varying the node mobility. It describes that increasing the speed of the mobile nodes, the E2E delay for the proposed system remains almost constant. It is obviously proves that the proposed NISD takes lesser E2E delay than the existing OLSR and AOLSR protocols.

The modified Dijkstra Algorithm reduces the size of the messages and reducing the overhead generated by maximizing the number of TC

messages. As the delay for 1-hop and E2E delay decreases, the average time taken is also reduced consequently. Hence, the proposed NISD takes lesser average time than the existing protocols which is shown in fig.9.

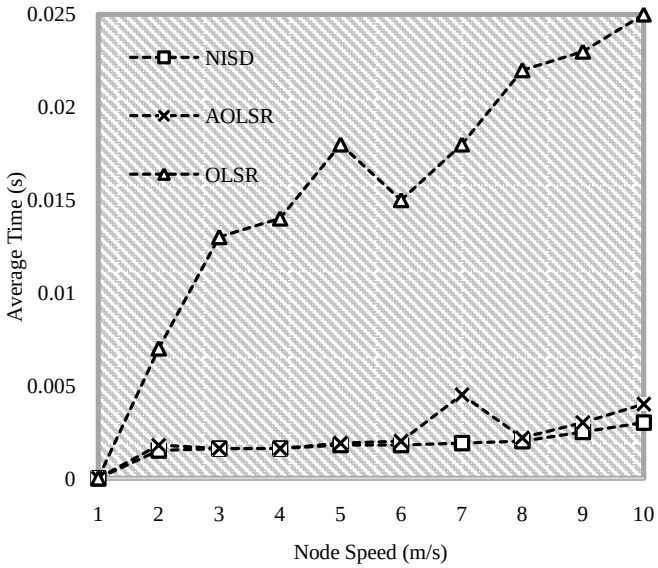

Fig.9: Simulations to compare the proposed NISD with existing OLSR and AOLSR against average time with varying node speed

All the protocols used in the simulation are analyzed based on the routing and security perspectives. Both the proactive and reactive protocols are vulnerable to malicious nodes, which interrupts the flooding of control traffic and data traffic information. Especially, the OLSR based routing protocols are affected by the incomplete view of the network topology structure. To the best of the proposed NISD, it increases the trusted communication with multiple disjoint paths.

Conclusion:

In this paper, an Intrusion Detection and Isolation System for OLSR protocol is introduced. NISD provides better security algorithms to ensure the trusted communication between the source and destination. The Modified Dijkstra Algorithm provides the flexible and scalable multiple disjoint paths between any two nodes of the network. Furthermore, NISD is compared with the existing OLSR and AOLSR protocols. With the presence of malicious nodes, the proposed method results above 80% packet delivery ratio. The experimental result shows that the proposed method outperforms than the existing method in terms of Packet Delivery Ratio, Delay, E2E delay and Average Time than the existing protocols even the presence of malicious nodes.

REFERENCES

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

Abdalla, A.M., I.A. Saroit, A. Kotband A.H. Afsari, 2011. "Misbehavior nodes detection and isolation for MANETs OLSR protocol," Procedia Computer Science, 3: 115-121.

Abdalla, A.M., I.A. Saroit, A. Kotb and A.H. Afsari, 2010. "An IDS for detecting misbehavior nodes in optimized link state routing protocol," in *2010 2nd International Conference on Computer Technology and Development (ICCTD)*, pp: 1-5.

Arifa Azeez, A.A., Elizabeth Isaac and SabuM Thampi, 2011. "Anonymous and Secured Communication Using OLSR in MANET," in *Advances in Computing and Communications*. vol. 193, A. Abraham, J. Mauri, J. Buford, J. Suzuki, and S. Thampi, Eds., ed: Springer Berlin Heidelberg, pp: 145-154.

Bose, D., A. Banerjee, A. Bhattacharyya, H. Saha, D. Bhattacharyya and P.K. Banerjee, 2012."An Efficient Approach to Secure Routing in MANET," in *Advances in Computing and Information Technology*. vol. 176, N. Meghanathan, D. Nagamalai, and N. Chaki, Eds., ed: Springer Berlin Heidelberg, pp: 765-776.

Cervera, G., M. Barbeau, J. Garcia-Alfaroand E. Kranakis, 2013. "Security issues in link state routing protocols for MANETs," in *Advances in Network Analysis and its Applications*, ed: Springer, pp: 117-148.

Chowdhary, M., S. Suri, and M. Bhutani, 2014. "Comparative Study of Intrusion Detection System.

Cervera, G., M. Barbeau, J. Garcia-Alfaro and E. Kranakis, 2010. "Mitigation of topology control

traffic attacks in OLSR networks," in *2010 Fifth International Conference on Risks and Security of Internet and Systems (CRiSIS)*, pp: 1-8.

Dhanalakshmi Natarajan and Alli P Rajendran, 2014. "AOLSR: hybrid ad hoc routing protocol based on a modified Dijkstra's algorithm," EURASIP Journal on Wireless Communications and Networking, pp:90.

Garg,N., K. Aswal and D.C. Dobhal, 2012. "A Review of Routing Protocols in Mobile Ad Hoc Networks," International Journal of Information Technology,l(5): 177-180.

Gao, Y., 2011. "Shortest path problem with uncertain arc lengths," *Computers & Mathematics with Applications*,62: 2591-2600.

Gawande, A., 2013. "Performance Analysis of DSR Protocol Under Sinkhole Attack in MANETs," International Journal of Research in Advent Technology,1.

Guo, Z., S. Malakooti, S. Sheikh, C. Al-Najjar and B. Malakooti, 2011. "Multi-objective OLSR for proactive routing in MANET with delay, energy, and link lifetime predictions," Applied Mathematical Modelling,35: 1413-1426, 3// 2011.

Hinds, A., S. Sotiriadis, N. Bessis and N. Antonopoulos, 2012. "Performance Evaluation of Security Algorithms for the AODV MANET Routing Protocol," presented at the Proceedings of the 2012 Third International Conference on Emerging Intelligent Data and Web Technologies.

Jiazi, Y., E. Cizeron, S. Hamma, and B. Parrein, 2008. "Simulation and Performance Analysis of MP-OLSR for Mobile Ad Hoc Networks," in *2008. WCNC 2008. IEEE Wireless Communications and Networking Conference*, pp: 2235-2240.

Lekova, A.and M. Adda, 2013. "Reliable OLSR in MANETs for detecting and isolating user selfish nodes," Complex Control Systems, 11: 1-9.

Marimuthu, M.and I. Krishnamurthi, 2013. "Enhanced OLSR for defense against DOS attack in ad hoc networks," *Journal of Communications and Networks*, 15: 31-37.

Rana, S.and A. Kapil, 2010. "Defending against Node Misbehavior to Discover Secure Route in OLSR," in *Information Processing and Management*. 70, V. Das, R. Vijayakumar, N. Debnath, J. Stephen, N. Meghanathan, S. Sankaranarayanan, *et al.*, Eds., ed: Springer Berlin Heidelberg, pp: 430-436.

Saroit, I.A.and A. Kotb, 2013. "Detection and Isolation of Packet Dropping Attacker in MANETs,"International Journal of Advanced Computer Science and Applications (IJACSA),4.

Shaw, S., K. Orea, P. Venkateswaranand R. Nandi, 2011. "Simulation and Performance Analysis of OLSR under Identity Spoofing Attack for Mobile Ad-Hoc Networks," in *Computer Networks and Information Technologies*. vol. 142, V. Das, J. Stephen, and Y. Chaba, Eds., ed: Springer Berlin Heidelberg, pp: 308-310.

Sun, Y., J. Sun, F. Zhao and Z. Hu, 2014. "Delay constraint multipath routing for wireless multimedia ad hoc networks," International Journal of Communication Systems.

Verbree, J.-M., M. de Graaf and J. Hurink, 2010. "An analysis of the lifetime of OLSR networks," *Ad Hoc Networks*, 8: 391-399.

Yi, J., A. Adnane, S. David and B. Parrein, 2011. "Multipath optimized link state routing for mobile ad hoc networks," *Ad Hoc Networks*, 9: 28-47.

Yi, J., E. Cizeron, S. Hamma, B. Parrein and P. Lesage, 2009. "Implementation of multipath and multiple description coding in OLSR," arXiv preprint arXiv:0902.4781.

Yi, J., S. David, H.A. Adnane, B. Parrein and X. Lecourtier, 2009. "Multipath OLSR: simulation and testbed," in 5th OLSR Interop/Workshop.

Zheng, S., T. Jiang, J.S. Baras, A. Sonalker, D. Sterne, R. Gopaul, *et al.*, 2008. "Intrusion detection of in-band wormholes in MANETs using advanced statistical methods," in *2008. MILCOM 2008. IEEE Military Communications Conference*, pp: 1-7.