# Integration of AODV and OLSR Routing Protocols for Providing Security in MANET's

**SEEMA KUMARI VERMA [#1], SATISH KUMAR YANAMADALA[#2]**

[#1] M.Tech Scholar, Department of CSE,
Chaitanya Engineering Collège, Kommadi, Visakhapatnam., AP, India.

[#2] Assistant Professor, Department of CSE,
Chaitanya Engineering Collège, Kommadi, Visakhapatnam., AP, India.

**ABSTRACT**

Network is a process of connecting multiple systems in order to transfer the information from one location to other location through some physical medium. There are mainly two types of networks: One is Client-Server Architecture (CSA) , in which a client will always have a facility like sending a request to the server and the server will always generates a response for that requested client. Another form is Peer to Peer (P2P) network in which each node can act as both sender and receiver. As we all know that the data or information in the network is mainly divided into packets of equal sizes. However during communication there may be occur some packets lost between nodes due to the reason like node or link failures created by the intruders. To protect these networks, security protocols have been developed to protect routing and application data. However, these protocols only protect routes or communication, not both. In this proposed thesis we try to propose an integrated approach to combine pre-existing routing approaches with security primitive and try to avoid data loss during communication. In this proposed thesis we try to find out the alternate path from the point of attack (POA) and optimize the packet delivery rate.

**Key Words:**

Packets, Data Communication, Node Failures, Routing Protocols, Point of Attack.

# I. Introduction

Now a day's almost each and every one is mainly concentrating on their data security. As we know that there was a huge demand and increase of using electronic devices by every user in order to store, retrieve, and access the data to and from electronic devices. There were a lot of hackers or intruders who try to hack or attack the sensitive data of others during data communication. This is the main problem in almost all the organization like banking, hotels, shopping malls, hospitals, schools and so on[1]. Generally attacks are classified into two types based on their individual roles and their individual functionality. They are as follows:

1. Physical Attack
2. Non-Physical Attack

Physical Attack is the process attempted by an intruder and in turn misuses the content or damage the content physically from its original content is known as physical attack. In this physical attack the data will not be transferred from valid source to valid destination, even some times with an attacked content [2]. On the other side if an attack occurs just in order to make delay during data transfer, without changing the original content is known as non-physical attacks. In this category the data will not be changed or damaged but just the data will be sending or received to and from the source and destination with some delay. Generally identifying the non-physical attack is very difficult for the network admin as the hacker can create delay either from source node or destination node or at router level. Hence it is very crucial task for the network admin to identify the non physical attacker [3].

From the below figure 1, we can clearly identify that the dos attack which is created on a distributed network is termed as a distributed denial of service attack and in turn they will try to deny the access of valid user from the target server. These DDOS attackers always try to deny the access of authorized users from the target server. As we all know that more delay always leads to loss, so if a DOS attacker who wish to create some disturbance in transmission of data to and from the target server, then it will be leads to data loss.DDoS also known as Distributed .In maximum cases, the owners of the zombie computers may not identify that they are being utilized or affected by attackers.

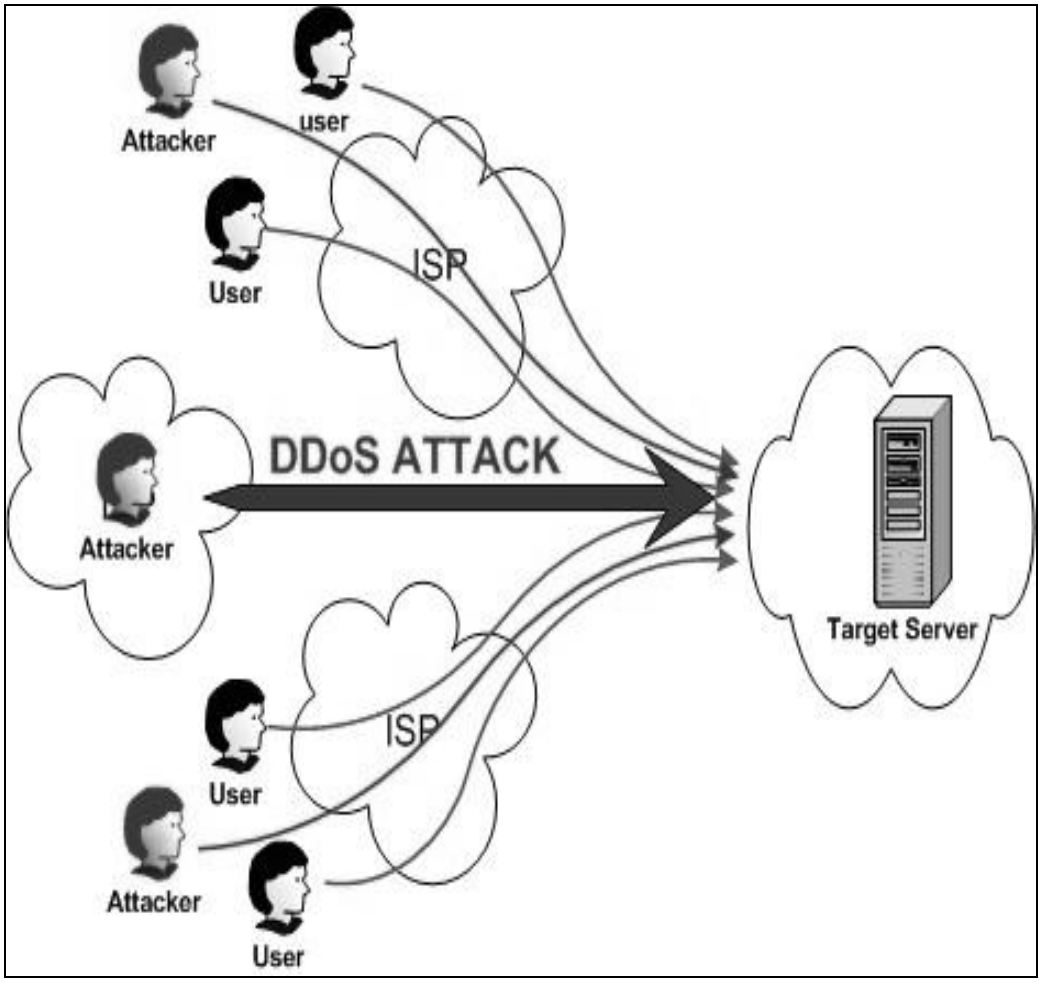


**Figure 1. Represents the Architecture of an DOS Attack**

From the above figure we can clearly identify that DDOS attackers try to create an disturbance in the network while the data is transferring and they will try to create some delay within the packets and once if more delay is occurred inside the network their will be loss of data transfer in the network[4].Hence in this proposed thesis we try to use integrated protocol in order to provide security over pre-existing routing approaches and also try to provide data access in an alternate way which don't give any attack[5]-[8].

## II. Related Work

In this section we mainly discuss about the related work that was carried out inorder to find out the proposed Integrated protocol. Now let us discuss about that in detail as follows:

**Motivation**

As we all know that for any data transfer from valid source to destination node, we need a network contain a set of nodes and edges with

$$G = (V,E),$$

Where 'G' is represented as a graph with

A set of vertices 'V' and

A set of edges 'E' between a pair of nodes like (u, v) such that nodes u and v can exchange messages between each other.

Here we try to assume that inter-node communication is symmetric in nature I.e. the key which is used for encryption at sender side should be used the same for the receiver side also. Generally an edge (u, v) is said to be incident on both the u and v nodes in the network. The nodes which are connected or having directly an edge with that node are known as the neighbors of node 'u'. Here we call a term like 'cut', which is the failure of a set of nodes Vcut from G results in G being divided into multiple connected components [6]. We can recall one thing that in an undirected graph 'G' is said to be perfectly connected if there is a way to go from every node to every other node by traversing the edges, and that a component Gc of a graph G is a maximal connected sub graph of G. We are interested in devising a way to detect if a subset of the nodes has been disconnected from a distinguished node, which we call the source node, due to the occurrence of a cut [9].

**AODV PROTOCOL**: Ad hoc on demand distance vector routing protocol

AODV is an on-demand routing algorithm in that it determines a route to a destination only when a node wants to send a packet to that destination. It is a reactive protocol. Routes are maintained as long as they are needed by the source. AODV is capable of both unicast and multicast routing. In AODV, every node maintains a table, containing information about which neighbor to send the packets to in order to reach the destination. Sequence numbers, which is one of the key features of AODV ensures the freshness of routes.

**OLSR PROTOCOL:** Optimized link state routing protocol

The Optimized Link State Routing (OLSR) is a table-driven, proactive routing protocol developed for MANETs. It is an optimization of pure link state protocols in that it reduces the size of control packet as well as the number of control packets transmission required. OLSR reduces the control traffic overhead by using Multipoint Relays (MPR), which is the key idea behind OLSR. A MPR is a node's one-hop neighbor which has been chosen to forward packets. Instead of pure flooding of the network, packets are just forwarded by a node's MPRs. This delimits the network overhead, thus being more efficient than pure link state routing protocols. OLSR is well suited to large and dense mobile networks. Because of the use of MPRs, the larger and more dense a network, the more optimized link state routing is achieved. MPRs helps providing the shortest path to a destination. The only requirement is that all MPRs declare the link information for their MPR selectors (i.e., the nodes who has chosen them as MPRs). The network topology information is maintained by periodically exchange link state information.

## III. Integration of AODV and OLSR Routing Protocols for Providing Security in MANET's

In this section we will mainly discuss about proposed approach for Integration of AODV and OLSR Routing Protocols for Providing Security in MANET's. Now let us discuss about this proposed model in detail as follows:

### Motivation

This paper proposes a novel security protocol for providing security for the data during communication. This proposed protocol try to combine routing and communication along with data security at the network layer. Here the data not only transfer under shortest path with valid source and destination but also looks at the alternate paths at the time of node failure or link failure[11].This proposed protocol try to give utmost security for the data which is send from source to destination under various attack cases.

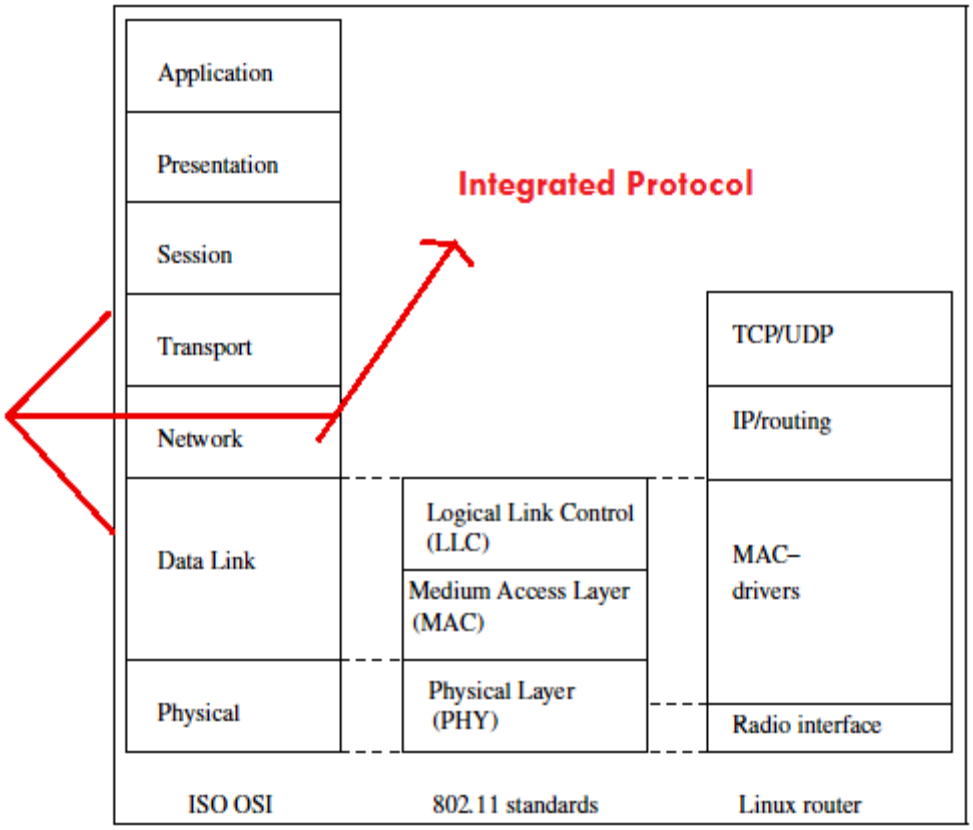


**Figure 2. Represents the Proposed Integrated Protocol Usage in OSI Model**

From the above figure 2, we can clearly identify that proposed integrated protocol is mainly present in the network layer to guide the data and packets which are attacked during transfer from advantages of the Proposed System data link to transport layer. Once if there is any attack occurred during this layer, the integrated protocol immediately invokes and tries to send the data in an alternate path from that POI (Point of Attack) node rather than sending the data all from the sender node. This will try to reduce a lot of delay and work load by sending the data from attacker node rather than from the starting node[12].

The Following are the some of the Advantages of our proposed approach. They are as follows:

1. Improve privacy of the network.
2. Increase data integrity.
3. Here the data confidentiality plays a major role.
4. Checks authenticity and integrity at each hop.
5. Provides solutions for the limitations that occur in two primitive routing techniques.

In order to overcome the problems in two existing routing protocols like AODV and OLSR,this integrated protocol came with an enhancement of security inside the two protocols like Secure Ad hoc On-demand Distance Vector (SAODV) and Secure Optimised Link State Routing (SOLSR) are secure implementations of AODV and OLSR respectively.SAODV secures the routing mechanism by including random numbers in Route Request packets (RREQs) [20]. If a routing packet arrives that re-uses an old packet number, that packet is invalid. Nodes observed sending re-played packets may be flagged as malicious. SAODV requires that at least two Secure RREQs (SRREQs) arrive at the destination node by different routes with identical random numbers to identify the source node.

## Control Messages in Integrated Protocol

Three message types are represented for data communication in a wireless adhoc networks. They are as follows:

RREQ : When a route is not available for the desired destination, a route request packet is flooded throughout the network.

RREP : It a node either is, or has a valid route to, the destination, it unicasts a route reply message back to the source.

RERR : When a path breaks, the nodes on both sides of the links issues a route error to inform their end nodes of the link break.

Here the proposed protocol will be in active state once if RERR is invoked during data transfer. This will be invoked if there is any attacker who try to create any attack inside the router, then this RERR is enabled and in turn that will activate the integrated protocol and hence the best alternate path is choose by that protocol to send the data without any loss.

## IV. Implementation Phase

Implementation is a stage where the theoretical design is automatically converted into programmatically manner by dividing the application into number of modules. The following application has mainly 3 modules with individual flow. Now let us discuss about these three modules in detail as follows:

1. System Configuration Module
2. Node Monitoring and Key Generation Module
3. Communication Security Module

### 1. System Configuration Module

In this module, the system construction is mainly done by initializing the sender, receiver and router and all these node details are updated in the database.

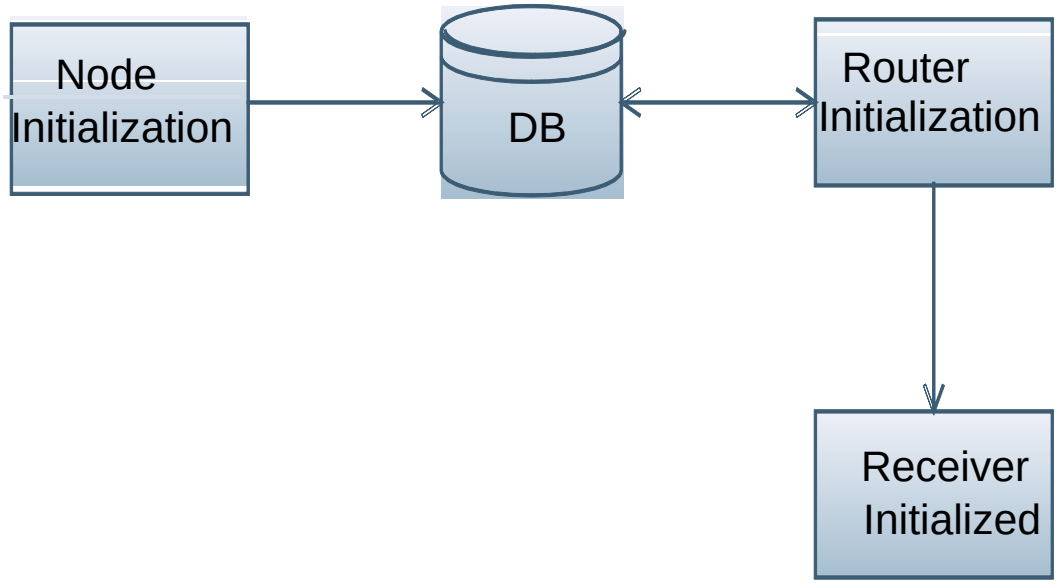


**Figure 3. Represents the System Construction Module**

### 2. Node Monitoring and Key Generation Module

Node monitoring is a collaborative detection strategy where a node monitors the traffic going in and out of its neighbors. Here the centralized key generator will try to generate a key for the set of nodes which are available on the router. So based on the path choose at the time of sending packets, these nodes try to exchange the information from sender to receiver node.

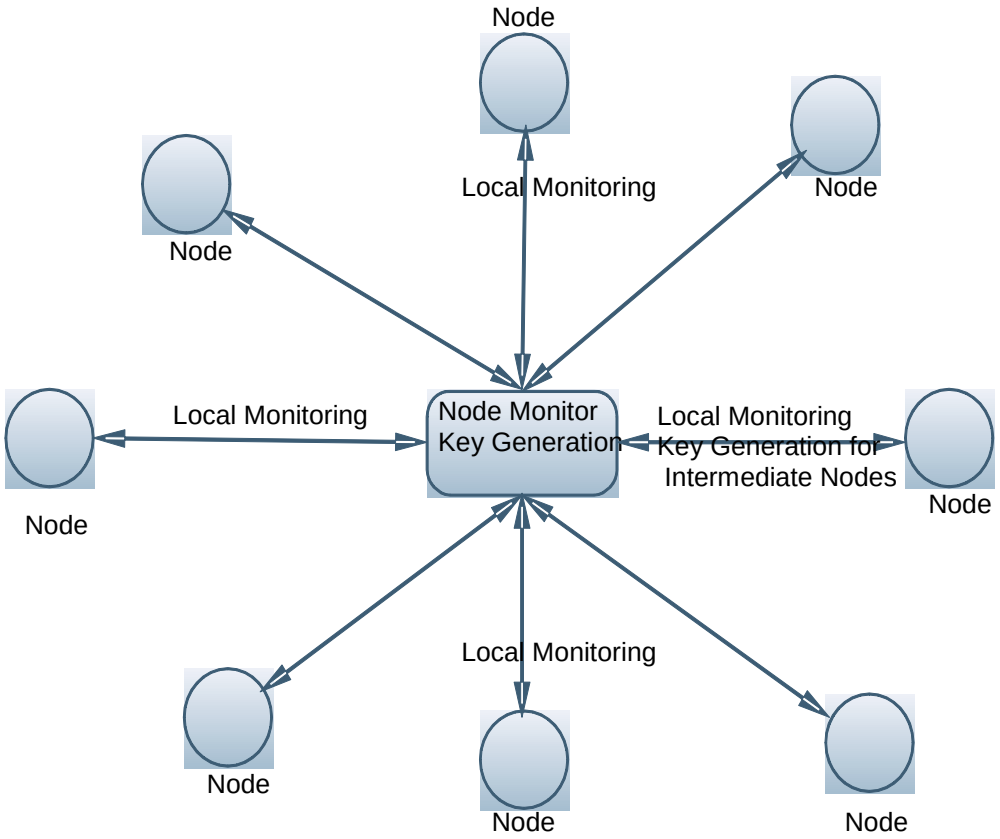


**Figure 4. Represents the Flow of Node Monitoring and Key Generation Module**

## 3. Communication Security Module

Along with its own sequence number and the broadcast ID, the source node includes in the REQ the most recent sequence number it has for the destination. During the process of forwarding the REQ, intermediate nodes record in their route tables the address of the neighbor from which the first copy of the broadcast packet is received, thereby establishing a reverse path. Once the REQ reaches the destination, the destination node responds by unicasting a route reply

packet back to the neighbor from which it first received the REQ. As the REP traverses along the reverse path, nodes along this path set up forward route entries in their route tables which point to the node from which the REP came. The changes to the basic version of AODV (Ad hoc On-Demand Distance Vector) is to enable the guard to build the necessary knowledge for detecting the energy or bandwidth attacks. In this proposed integrated protocol we will detect the attack nodes and avoid sending data through those nodes.

## V. Conclusion

In this proposed thesis we for the first time developed an integrated approach to combine pre-existing routing approaches with security primitive and try to avoid data loss during communication. As we all know that the data or information in the network is mainly divided into packets of equal sizes. However during communication there may be occur some packets lost between nodes due to the reason like node or link failures created by the intruders. To protect these networks, security protocols have been developed to protect routing and application data. However, these protocols only protect routes or communication, not both. In this proposed thesis we try to propose an integrated approach to combine pre-existing routing approaches with security primitive and try to avoid data loss during communication. In this proposed thesis we try to find out the alternate path from the point of attack (POA) and optimize the packet delivery rate.BY conduction various experiments on our proposed approach we finally came to an conclusion that our proposed approach is best in providing security for the data and avoid data or packet loss during communication.

## VI. References

[1] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in mobile ad hoc networks: challenges and solutions,” *Wireless Communications, IEEE*, vol. 11, no. 1, pp. 38– 47, 2004.

[2] N. Garg and R. Mahapatra, “Manet security issues,” *IJCSNS*, vol. 9, no. 8, p. 241, 2009.

[3] .U. D. Khartad and R. K. Krishna, "Route Request Flooding Attack Using Trust Based Security Scheme in Manet," International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), Vol. 1, No. 4, 2012, p. 27.

[4] P. Gupta and N. Mckeown, "Classification using hierarchical intelligent cuttings," *IEEE Micro*, vol. 20, no. 1, pp. 34–41, Jan.–Feb. 2000.

[5] H.Lim,H.Chu, andC. Yim, "Hierarchical binary search tree for packet classification," *IEEE Commun. Lett.*, vol. 11, no. 8, pp. 689–691, Aug.2007.

[6] I. D. Chakeres and E. M. Belding-Royer, "Aodv routing protocol implementation design," in *Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on*. IEEE, 2004, pp. 698–703.

[7] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot *et al.*, "Optimized link state routing protocol (olsr)," 2003.

[8] B. Lampson, B. Srinivasan, and G. Varghese, "IP lookups using multiway and multicolumn search," *IEEE/ACM Trans. Netw.*, vol. 7, no. 3, pp. 324–334, Jun. 1999.

[9]. R. Guo, G. R. Chang, R. D. Hou, Y. H. Qin, B. J. Sun, A. Liu, Y. Jia and D. Peng, "Research on Counter Bandwidth Depletion DDoS Attacks Based on Genetic Algorithm.

[10] S. Dharmapurikar, H. Song, J. Turner, and J. Lockwood, "Fast packet classification using Bloom filters," in *Proc. ACM/IEEE ANCS*, 2006,pp. 61–70.

[11] M. Hyland, B. E. Mullins, R. O. Baldwin, and M. A. Temple, "Simulation-based performance evaluation of mobile ad hoc routing protocols in a swarm of unmanned aerial vehicles," in *Advanced Information Networking and Applications Workshops, 2007.*

[12] J. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, "Performance analysis of mesh routing protocols for uavswarming applications," in *Wireless Communication Systems (ISWCS), 2011 8th International Symposium on*. IEEE, 2011, pp. 317–321.

## VII. About the Authors

**SEEMA KUMARI VERMA** is currently pursuing her 2 Years M.Tech in the Department of Computer Science and Engineering at Chaitanya Engineering College, Kommadi, Visakhapatnam., AP, India. She completed her B.Tech in information technology at Annamalai university, Chidambaram Tamil Nadu..His area of interest includes the Networking, Mining and Software Testing.

**SATISH KUMAR YANAMADALA** is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Chaitanya Engineering College, Kommadi, Visakhapatnam., AP, India. He has more than 6 years of teaching experience in various engineering colleges. His research areas include the Image Processing.