# Modified Ad-Hoc On-Demand Distance Vector Routing Algorithm: An era of transformation in conventional AODV

Amandeep Kalra[1], Dr. S. S. Khurmi[2]
*[1]Research Scholar*
*[2]Professor*
*Desh Bhagat University, Mandi Gobindgarh*

**Abstract:** Over wireless sensor network (WSN), several routing algorithms are studied and analysed around the globe. Certain algorithms create a benchmark in deployment of network effectively. AODV routing algorithm is a reactive protocol in which nodes respond as per the demand arises. Networks don't keep up directing data or action in the system hub if there is no correspondence. But several shortcomings have been analysed during the study of this routing algorithm. In this paper, authors have tried to achieve Modified AODV where conventional AODV is curbed to attain better results in a network.

**Keywords:** Wireless Sensor Networks (WSN), Ad-hoc On-Demand Distance Vector Routing algorithm (AODV), Routing Algorithms, Blackhole attack.

## I. INTRODUCTION

Wireless Sensor Network consists of small and light weighted large number of wireless nodes called sensor nodes with the ability to communicate among themselves and also to an external sink or a base-station to form a communication network such as a single multi-hop network or a hierarchical organization with several clusters and cluster heads. These sensors are deployed in physical or environmental condition to measure physical parameters such as sound, pressure, temperature, humidity, etc. Wireless sensor networks (WSNs) have been used for numerous applications including habitat monitoring, building monitoring, health monitoring, military surveillance, target tracking, etc. Generally, WSN have broad applications in either controlled environments (such as home, office, warehouse, etc) or uncontrolled environments (such as hostile or disaster areas, toxic regions, etc). Some important applications are: Area monitoring i.e., gathering information from a region where it is located. Environmental monitoring i.e., measurement of temperature, rainfall etc.[1]

Recent advances in wireless sensor networks have led to many new protocols specifically designed for sensor networks where energy awareness is an essential consideration. Most of the attention, however, has been given to the routing protocols since they might differ depending on the application and network architecture.[2]

Ad-Hoc On-demand Distance Vector Routing (AODV): It is a reactive protocol or on-demand protocol. AODV protocol uses destination sequence number to offer loop-free routing and fresh route to the destination. Unlike tables driven protocols it does not maintain status of the network via continuous updates. This approach helps in reducing the number of messages and the size of the routing tables. AODV provides both multicast and unicast connectivity in an Ad-Hoc environment. One of the main feature of AODV is to respond quickly whenever a link breakage in active route is found. AODV is a combination of both DSR and DSDV. It inherits the basic on-demand mechanism of route discovery and route maintenance from DSR plus the use of hop-by-hop routing sequence numbers and periodic beacons from DSDV.[3]

## II. LITERATURE SURVEY

A number of state-of-the-art reviews exist today in WSNs, covering from broad to specific areas of interest. However, a comprehensive review on secure routing issues in WSNs appears to be missing. Also in developing country like India, economical networking is very important.

Eliana Stavrou and Andreas Pitsillides [4] have reviewed the WSN multipath routing protocols. But they have not take into consideration the attacks that can greatly influence the network when launched from inside adversaries, e.g. wormhole, sinkhole, hello attacks. These attacks are usually more difficult to defeat because the adversary has already gained access and is considered as a part of the network.

M. Saleema, G. Di Carob, and M. Farooqc [5] have reviewed the swarm intelligent based routing protocols in WSN and a suggested a new framework. The proposed framework consists of five top level modules and some additional sub-modules. The ensemble of these modules and sub-modules implements the architecture and the operations at the node router. The top level modules are: (i) mobile agent generation and management, (ii) Routing Information Database (RID), (iii) agent structure, (iv) agent communications and (v) packet forwarding.

J. Barbancho, C. Leon, F. Molina, and A. Barbancho.[6] proposed a new AI-based routing algorithm for WSN. This algorithm is called Sensor Intelligence Router (SIR) which has the novelty of being based on the introduction of neural networks in every sensor node. The wireless sensor network simulator, OLIMPO, have been carried out to study the efficiency of the proposed protocol. SIR was designed to flat-based routing network where all nodes are supposed to be assigned equal roles or functionalities. Among all the existing flat routing protocols, they have chosen directed diffusion and Energy-Aware Routing (EAR) to evaluate the influence of the use of AI techniques.

Some other researchers have been made attempts using genetic algorithms to solve some WSNs problems like Hussain et al (2007), Jin et al (2005), Ferentinos and Tsiligiridis (2007), Wazed et al (2007), Rah-Mani et al (2006) and Qiu et al (2006). Despite these efforts most of the problems of WSNs using genetic algorithms remain unexplored. No work has been done to addresses secure routing in WSN using GA.

## III. PROPOSED FRAMEWORK

The proposed framework as shown in figure 1 determines the main phases that will be followed in order to create a new AI-based routing protocol for WSN. There are three main phases: Design phase, testing phase, and performance measurement phase. Each of these steps contains a set of tasks. Each task can be understood from its name as shown in figure.

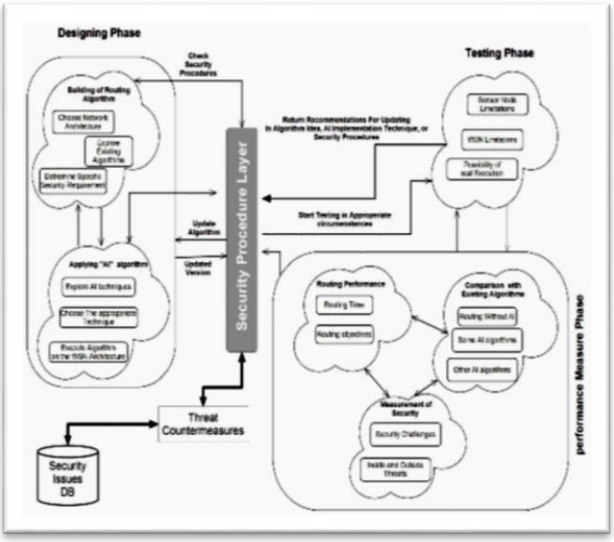
Designing Phase
Check Security Procedures
Building of Routing Algorithm
Choose Network Architecture
Explore Existing Algorithms
Determine Specific Security Requirement
Testing Phase
Sensor Node Limitations
WSN Limitations
Feasibility of real Execution
Return Recommendations For Updating in Algorithm Idea, AI Implementation Technique, or Security Procedures
Security Procedure Layer
Start Testing in Appropriate circumstances
Update Algorithm
Updated Version
Applying "AI" algorithm
Explore AI techniques
Choose The appropriate Technique
Execute Algorithm on the WSN Architecture
Routing Performance
Routing Time
Routing objectives
Comparison with Existing Algorithms
Routing Without AI
Some AI algorithms
Other AI algorithms
Measurement of Security
Security Challenges
Inside and Outside Threats
performance Measure Phase
Threat Countermeasures
Security Issues DB

**Figure 1: The Proposed Framework**

Key exchange mechanism will be used to achieve security.

### THE PROPOSED SOLUTION

In this section, propose a methodology for identifying black hole nodes with slightly modified AODV protocol. The solution that propose here is designed to detect the Blackhole nodes in the default operations of either the intermediate nodes or that of the destination nodes. The approach follow, basically modifies the working of the source node and the change of the functioning of route reply using function broadcast the route reply (same like the route request function). In this proposed solution using a method called Prior_ReceiveReply. In this method three things are added, a new table Reply-Table (Request Reply), a timer WT (Waiting Time) and a variable hackerNode (Malicious Node ID) to the data structures in the default AODV Protocol.

The main benefits of modifying the AODV protocol is (1) the malicious node is identified at the initial stage itself and immediately removed so that it cannot take part in further process. (2) With no delay the malicious node are easily identified i.e. as said before all the routes has unique sequence number. Generally the malicious nodes have the highest Destination Sequence number and it is the first RREP to arrive. So the comparison is made only to the first entry in the table without checking other entries in the table. (3) No modification is made in other default operations of AODV Protocol (4) Better performance produced in little modification.

## IV. CONCLUSION

A new protocol has been developed which is based on existing AODV. As the topic of the research is to provide security and stability in MANET. So in the proposed algorithm both these issues are taken into account. It is basically the enhancement of the existing AODV algorithm as it provides better stability in normal working and provides security from wormhole attack in network.

In new algorithm has been proposed named as Modi_AODV. This algorithm is basically the enhanced or better algorithm in comparison of existing AODV. Here, NS2.32 simulator on Fedora 13 is used for the measurement of the results between existing AODV and Modi_AODV. The results shows clearly that Modi_AODV is better and giving stable performance in the proposed Modi_AODV but it will increase the overhead control packets. The propose algorithm is capable of not only detecting the wormhole attack but also it will deactivate the participation of the wormhole nodes in MANET.

## V. FUTURE WORK

The work still requires a lot to be done in the field of maintaining power energy of the nodes, cryptography and to control the overhead packets. More denser and sparse real life scenarios are needed for the protocol to be robust in nature. More comparisons are required with other schemes like DSR, TORA. Power feature can also influence the study further.

## VI. REFERENCES

[1]. S. Desai, S. Butani and S. Valiveti, "Analyzing The Impact Of Standard Encryption Approaches For Data Aggregation In A Wireless Sensor Network", International Journal of Computer Science and Telecommunications, Volume 3, Issue 6, June 2012.

[2]. K. Akkaya and M. Younis, "A Survey Of Routing Protocols In Wireless Sensor Networks And Ad Hoc Network", Elsevier Journal, Volume 3 , Issue 3 , 2005.

[3]. M. K. Marina and S. R. Das,"Ad Hoc On-Demand Multipath Distance Vector Routing", Wireless Communications and Mobile Computing, ISSN:1530-8677 (online), Vol. 6, Issue 7, pp. 969-988, 2006. DOI: 10.1002/wcm.428.

[4]. E. Stavrou and A. Pitsillides, " A Survey On Secure Multipath Routing Protocols In WSNs", Computer Networks, Volume 54, Issue 13, September 2010.

[5]. M Saleema, G. Di Carob, and M. Farooqc, "Swarm Intelligence Based Routing Protocol For Wireless Sensor Networks: Survey And Future Directions", Information Sciences, Volume 181, Issue 20, October 2011.

[6]. J. Barbancho, C. Leon, F. Molina and A. Barbancho,"Using Artificial Intelligence In Routing Schemes For Wireless Networks", Computer Communications, Volume 30, No.14-15. October 2007.