International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

# A Survey of Protocols Enhancing the Security and Performance of AODV

**Mahima Sharma[1], Ankita Singh[2]**

[1, 2] School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India

**Abstract:** ***MANET (Mobile Ad Hoc Networks) is a collection of mobile devices such as laptops, mobiles, etcetera that communicate with each other without an access point. Since the devices are on the move, the topology of the MANET keeps on changing. Due to various inherent as well as circumstantial issues of MANET, routing protocols lack in features such as Security, Performance and Power consumption. Ad-hoc On-Demand Distance Vector (AODV) Routing is a reactive routing protocol for MANET. The pitfall of this algorithm is that it wasn't built keeping security in mind. Several modifications in the protocol have been proposed and impl emented to improve its security and performance. This paper aims at presenting a comparative study of some of the approaches presented to enhance AODV's security and performance. For example: Hashing, Key Management, AODV-AD, IMAODV, Zonal Routing (AODV).***

**Keywords:** MANET; AODV; Reactive Routing Protocol; Hashing; Key Management; AODV-AD; IMAODV; Zonal Routing

## 1. Introduction

MANET is a collection of independent mobile users or nodes that communicate over relatively bandwidth and power constrained wireless links. These networks are built, work and maintained by its own because each node performs dual role of host and router. By and large, these nodes have a limited transmission range and so each node search for the support of its neighboring nodes in forwarding packets. [1] The data is transferred in multi-hop manner. Due to ever changing location of nodes the topology of MANET keeps on changing. The absence of access point makes the network self-configuring. They are also subject to frequent disconnection during node's mobility. In addition, wireless links have been significantly affected by constrained resources such as bandwidth and power [2].

In recent years mobile ad hoc networks (MANETs) have received tremendous attention because of their self-configuration and self-maintenance capabilities. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. The unique characteristics of MANETs present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints and highly dynamic network topology. Consequently, the existing security solutions for wired networks do not directly apply to the MANET domain. The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users [3].

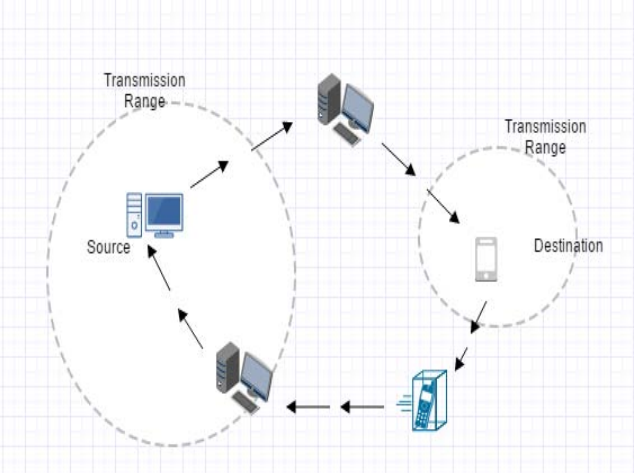


**Figure 1:** Structure of MANET

The above shown figure depicts the structure of MANET and the way in which packets flow between source and destination. The routing for MANET is way different from wired networks. In contrast to traditional network routing protocols, for example for wired networks, the behavior of ad hoc networks can be quite dynamic due to factors such as node movement and variations in radio propagation condition, creating frequent changes in network topology, differing concentration in traffic load on the network, and other challenges to the operation of the network protocols, and thus must adapt more quickly [25]. These challenges make routing for MANET a bit complicated. There has been a lot of research in this area from the 90's. Routing scheme in MANET governs how connections are established, how data is transferred and the error handling procedures.

There are three approaches for routing in MANETs: Proactive, Reactive and Hybrid. Proactive or Table Driven approach aims at creating detailed and updated routing information for all the nodes. Protocols such as link-state, DSDV [15], OSLR [10] are proactive routing protocols. The overhead for such protocols is quite high. Reactive approach also known as On-Demand routing creates routes between two nodes only when either of the two wishes to communicate with the other node. This type of protocols doesn't incur high overhead. AODV, DSR [16] and TORA

[17] are examples of reactive routing protocols. Hybrid routing protocols such as ZRP [5] and SLSP [18] combine the best features of both reactive and proactive routing protocols. For example, a node communicates with its neighbors using a proactive routing protocol, and uses a reactive protocol to communicate with nodes farther away. [2]

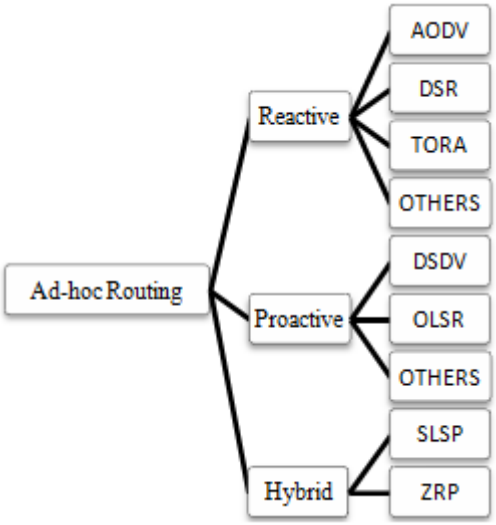


**Figure 2:** Types of Routing Methodologies for MANET

The next section of the paper focuses on AODV protocol. A short description of the advantages and disadvantages of the protocol will also be given. In the further sections a review of some of the works published for enhancing the performance of AODV will also be given.

## 2. AD-HOC on-Demand Distance Vector (AODV) Routing

AODV is a reactive routing protocol which works on On-Demans basis. It creates path only when it is required to do so. When a source node wishes to communicate to a destination node, a route is generated for the same. This route however would not be generated until and unless the source wishes to communicate. The routing information is stored on all the nodes that are responsible for communication and the nodes that are on active route of communication. AODV does not maintain any list for nodes that are not on the active path. In case of a broken link it propagates this message to the neighbors. Each node has its own unique Sequence ID and Broadcast ID. The routing packets contain respective Sequence ID of the destination. This ensures loop free communication.

AODV has three main phases: path identification, route establishment and maintenance. AODV is a standard routing protocol for MANETs. It has low overhead & low resource consumption. AODV routing protocol is widely used in Mobile Ad hoc networks, but it does not have any security mechanism, so it is very vulnerable to security attacks. [6] AODV is totally based on distance vector routing process in MANET. When security mechanism is applied to it, the performance of the whole network degrades. [4] Despite of its various merits, AODV lacks security. It was initially designed with no security aspect.

There have been several modifications in AODV that have been suggested to improve the security aspect without compromising the overall performance of the protocol. In the next section, a small review of various approaches is given.

## 3. Security Issues of Ad-Hoc Networks

The Ad-hoc networks due to their decentralized architecture are prone to various types of attacks. The nodes move freely, resources are constrained and the authenticity of nodes is difficult to access. This adds up to make the problem even worse. MANETs use shared broadcast medium for transmission. While delivering data to multiple destinations, multicast communication is of great concern in these networks, since it helps saving resources. While transmission, there are chances that the route gets busy due to greater traffic or some node may fail which rush the traffic to other nodes which can be the cause of congestion. So, it is important to avoid congestion collapse in wireless multi-hop networks in order to perform efficient congestion control [9]. MANET is primarily used in military information system of battle field, civil emergency search-and-rescue operations and other occasion. [7] A slight glitch in security in such areas can cause excessive damage. The security of MANET is therefore an important aspect that cannot be ignored.

The attacks on MANET can be classified into two broad categories:

- Passive Attacks
- Active Attacks

Passive Attacks: Passive attacks are those attacks that do not alter the network information however they might cause a threat to the information by extracting it. A certain node might become malicious and stop performing the task it is supposed to perform.

Passive Attacks can be further classified into: Eavesdropping and Traffic analysis. Eavesdropping is that attack in which malicious node overhears the communication between two nodes. Traffic analysis attacks occur when the data flow is being accessed. The data packets are tapped and stored by the attacker. These messages can then be interpreted.

Active Attacks: Active attacks can cause a bigger threat to the network by altering or damaging the information being sent across the network. These attacks can be further classified into: Dropping attacks, Modification attacks, Fabrication attacks and Timing attacks. Dropping attacks are those in which the data packets are dropped by the malicious nodes. Modification attacks are those in which data packets are altered during the process of communication. Fabrication attacks are those attacks in which the node forges the messages. Timing attacks are those in which the malicious nodes show wrong newer routes to the destination.

The AODV protocol has been modified or enhanced in various projects to withstand some or all of these attacks. The major problem with AODV is that its performance degrades very rapidly when security is tried to improve.

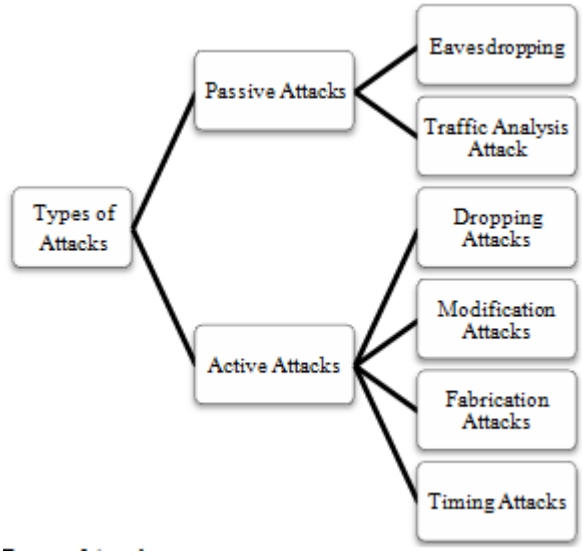


**Figure 3:** Types of Attacks

## 4. Performance Measures of A Routing Protocol

There are various measures for studying the effectiveness of a routing protocol. These measures when applied to a routing protocol enable us to adjudge efficiency of their mechanism. Some standard measures of performance are:

a) Packet Delivery Ratio: It is defined as the ratio of total number of packets being delivered to the total number of packets being generated by the system.
b) Throughput: The total number of packets transmitting through the channel and reaching the destination is defined as throughput of the system.
c) Routing load: We very well know that not all packets reach their destination. Thus, for every packet that gets delivered, routing load is defined as total number of packets sent out.
d) Average End to End Delay: It is defined as the time span between the generation of first request packet and last bit of information being sent.
e) Routing Overhead: Routing Overhead: When nodes change their location within network, some extra routes get generated in the routing table. These routes generate unnecessary overhead. This is known as routing overhead [9].

These measures are used to analyze the performance of modified protocols with reference to original protocol. There have been many modifications to the AODV protocol. Some of the research work for modification or enhancement of AODV is analyzed and briefed in the next section.

## 5. Survey of Works Proposed that Improve AODV's Security

a) AODV-AD [7] AODV is enhanced or improved upon by implementing or enforcing attack detection with it. Attack detection is implemented upon by using credence mechanism, adjudges a malicious node as an attacker and isolates it. This algorithm modifies AODV by adding features like Black Hole Detection, Routing Table Overflow Attack, Fabricating Reply Packet Attack Detection and Interrupt Routing Attack. This algorithm improves AODV's overall performance by choosing route with higher credence value while performing routing. The nodes perform this process on their own.
After simulation analysis under NS2, it is proved that the performance of the revised AODV protocol is better than before, which makes Ad Hoc networks safer and enhances the availability. [7]

b) AOZDV [5] A modified AODV approach, in which the effectiveness of AODV is incremented by implementing zone routing. This approach identifies the drawbacks of route discover process in large MANETS.
The algorithm works by implementing Zone Routing Protocol with AODV. A node creates its own zone with all the neighboring nodes on the basis of traffic and power information.
AOZDV constructs a zone at the source and the destination based on its traffic and power information, and builds DVT for routing in the zone. For building a path from the source to the destination, the AODV algorithm is used to reach the Destination Zone, and ZRP is adopted to find the destination in the Destination Zone[5]. Simulations proved that this approach is better than AODV.

c) AODV-LAR[22]: AODV-LAR has been derived from Line Aided Routing (LAR) Protocol. This protocol makes use of Global positioning system to identify locations of source and destination nodes. The distance is then used to inhibit nodes from flooding AODV. In this protocol, the Geo Positioning System is used to identify the locations of each node. These positions are then sent with each message from that node in piggybacking manner. Thus, the overhead of route discovery is minimized.
This protocol mainly aims at reducing the overhead of messages sent by AODV protocol. On performing simulations, this protocol shows improvement over AODV in terms of control overhead, delay and delivery ratio.

d) IMAODV [8] Improved Multicast Ad-hoc On Demand Distance Vector is a shared tree based approach. each multicast group has its own shared tree. When a node is arrives, it is added to a multicast tree for that group. This tree is bi-directional. Each group has its own leader that maintains all routing information for that group. It enables dynamic, self-starting, multihop routing between participating mobile nodes in wishing to join or participate in a multicast group within an ad hoc network. [8] This approach has low overhead, it can easily recover from situations like link breakage and the response is faster.
By simulations, it was proved that Packet Delivery ratio was much higher in case of IMAODV as compared to AODV.

e) Securing AODV using Encryption Techniques: AODV can be secured by using various Encryption techniques such as RSA [19], DES [20], AES [20], Digital Signature [24] and IDEA [21]. They are the solutions for implementing Security Mechanisms in AODV. A paper

published in 2015, by Jagdale and Patil, secured the AODV by implementing it with various encryption techniques. The various algorithms used were RSA-AODV [14] and AES-AODV [14] among others.
Simulations were performed to assure that the new protocols withstand attacks on the network. The protocol is based on group signature and ID-based cryptography and two phases anonymous key establishment, privacy preserving secure routing. [14]
The work on these protocols still continues to enhance the performance aspect.

f) Securing AODV using HASH Function [13]: A lot of work has been published for securing AODV using HASH function. A paper published in 2013, by Soni & Nayak, aims at improving the security of AODV by integrating HASH Chain Function and Digital Signature. The AODV messages are secured by calculating digital signature for the un-modifiable part of the AODV message. Then a hash chain function is applied to the modifiable part of the AODV message. This method also enabled the protocol to defend itself against malicious and unauthenticated nodes.

g) RB-AODV [23]: Receiver Based AODV works on the principle of AODV but in reverse. The route discovery process is initially similar to that of AODV. The only difference is that the destination will broadcast Request Packets to the source. The route discovery is performed in opposite manner. This way the source will always have newer and most recent routes to the destination. In case of link breakage or any other error, the nodes on the active path instead of generating error packets, choose the latest active path.
The simulation results show that RB-AODV produces a better performance in terms of end-to-end delay, packet delivery ratio, and control overhead compared to the AODV protocol [23].

h) SECURITY ADAPTIVE PROTOCOL SUITE [25]: This protocol suite uses two approaches Ranked Neighbor Discovery (RND) and Security Adaptive Ad-Hoc On-Demand Distance Vector (SAAODV) routing algorithm. The suite has two phases: the first phase is neighbor discovery and the second phase is security based routing. In the first phase, the main focus is to generate a list of trusted neighbors. These trusted neighbors are then ranked on the basis of some factors. According to this a trust ranking is obtained. In the second phase, AODV due to its various merits is chosen for routing process. It is secured to form SAAODV. The routing is similar to that of AODV. The only difference is defining of a security level. On the basis of trust ranking the nodes for active route are chosen. The broadcast packets will not be sent to nodes with lower trust ranking. Thereby, reducing the risk of packets being accessed by intruders. The rest process remains same. The suite can identify wormholes and remove them.
The proposed model is only a theoretical model, designed with the main objective of focusing on the security issues of a wireless environment [25].

## 6. Conclusion

The main aim of this paper is to give an insight into an ever evolving area of research "MANET". AODV is a standard routing protocol for MANET. There are, however, some security issues in AODV that need to be addressed. When these security issues are taken care of the overall performance of the network goes down. Various performance metrics were also listed down in this paper. The performance of a protocol can be adjudged on the basis of these metrics. This paper presents a brief overview of some approaches that enhance or improve the security of existing AODV protocol. The approaches are theoretical as well as practically proven on some simulation tools. Each approach has its own way of addressing the issues. The approach and the results of the simulation performed, if any, are mentioned with them. There is always scope for improvement in every approach. Here we aim at only briefing their working and the performance of the improved protocols as opposed to the original one.

## References

[1] Sunil J. Soni and Suketu D. Nayak "Enhancing Security Features & Performance of AODV Protocol under Attack for MANET" 2013 International Conference on Intelligent Systems and Signal Processing (ISSP).
[2] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani "A Survey of Secure Mobile Ad Hoc Routing Protocols" IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 10, NO. 4, FOURTH QUARTER 2008.
[3] Rakesh Kumar Jha, Suresh V. Limkar and Dr. Upena D. Dalal "A Performance Comparison of Routing Protocols for Security Issue In Wireless Mobile Ad Hoc Networks" Third International Conference on Emerging Trends in Engineering and Technology 978-0-7695-4246-1/10 2010 IEEE.
[4] Morli Pandya & Ashish Kr. Shrivastava "Improvising the Performance with Security of AODV Routing Protocol in s" 2013 Nirma University International Conference on Engineering (NUiCONE).
[5] HongKi Lee, YongWoo Kim and JooSeok Song "AOZDV: An Enhanced AODV Protocol based on Zone Routing in MANET" 1-4244-1312-5/07 2007 IEEE.
[6] Zhang Guoqing, Mu Dejun, Xu Zhong and Yang Weili "An Efficient Security Enhancement of AODV Protocol" Proceedings of the 26th Chinese Control Conference July26-31, 2007.
[7] Liu Jun, Li Zhe, Lin Dan and Liu Ye "A Security Enhanced AODV Routing Protocol Based On the Credence Mechanism" 0-7803-9335-X/05 2005 IEEE.
[8] Srinivas Sethi and Siba K. Udgata "IMAODV: A Reliable and Multicast AODV Protocol for MANET" 978-1-4244-5875-2/09 2009 IEEE.
[9] Bandana Bhatia "Performance Analysis of AODV Based Congestion Control Protocols in MANET" 2015 1st International conference on futuristic trend in computational analysis and knowledge management (ABLAZE 2015).

[10] P.Jacquet,T.Clausen,A.Qayyum,and L.Viennot," Optimized Link State Routing Protocol for Ad-hoc Networks".
[11] Keita Matsuo, Tetsaya Oda, Donald Elmazi, Shinji Sakamoto and Leonard Barolli "Performance Evaluation of AODV, OLSR and HWMP Protocols In Ad-Hoc Networks and MANET Scenarios" 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing.
[12] Abdulaziz AI-Nahari, Mohd Murtadha Mohamad and Saleh AI-Sharaeh "Receiver-Based AODV Routing Protocol for MANETs" 978-1-4799-3516-1I13 2013 IEEE.
[13] Wenqi Yu "A Pairwise Key Management Scheme Based on Hash Function for Wireless Sensor Networks" 2010 Second International Workshop on Educational Technology and Computer Science.
[14] Prof. B. N. Jagdale and Mrunal S. Patil "Emulating Cryptographic Operations for Secure Routing in Ad-hoc Network" 2015 International Conference on Pervasive Computing (ICPC).
[15] Khaleel Ur Rahman Khan, A Venugopal Reddy, Rafi U Zaman, K. Aditya Reddy and T Sri Harsha "An Efficient DSDV Routing Protocol for Wireless Mobile Ad Hoc Networks and its Performance Comparison " Second UKSIM European Symposium on Computer Modeling and Simulation 978-0-7695-3325-4/08 2008 IEEE DOI 10.1109/EMS.2008.11.
[16] Thouraya Bouabana-Tebibel "A secure routing scheme for DSR" 2011 First ACIS International Symposium on Software and Network Engineering.
[17] Asad Amir Pirzada and Chris McDonald "Trusted Route Discovery with TORA Protocol" Proceedings of the Second Annual Conference on Communication Networks and Services Research (CNSR'04) 0-7695-2096-0/04 2004 IEEE.
[18] Panagiotis Papadimitratos and Zygmunt J. Haas "Secure Link State Routing for Mobile Ad Hoc Networks" .
[19] Kartik Kumar Srivastava, Avinash Tripathi and Anjanesh Kumar Tiwari "Secure Data Transmission in AODV Routing Protocol" International Journal of Communication and computer Technologies Volume 01 – no.18, Issue: 04 April 2013.
[20] William E. Burr "Selecting the Advanced Encryption Standard" 1540-7993/03 2003 IEEE.
[21] Wen-Xiang Zhang,Si-You Xiao and Yi Zhang "Research on Image-text Encryption Techniques in Mobile Communications" 2010 Second WRI Global Congress on Intelligent Systems.
[22] Mohannad Ayash, Mohammad Mikki and Kangbin Yim "Improved AODV Routing Protocol to Cope With High Overhead in High Mobility MANETs" 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing.
[23] Abdulaziz AI-Nahari, Mohd Murtadha Mohamad and Saleh AI-Sharaeh "Receiver-Based AODV Routing Protocol for MANETs" 978-1-4799-3516-1I13 2013 IEEE.
[24] Raghav Mathur, Shruti Agarwal and Vishnu Sharma "Solving Security Issues in Mobile Computing using Cryptography Techniques -A Survey" International Conference on Computing, Communication and Automation (ICCCA2015).
[25] Rasib Hassan Khan , K. M. Imtiaz-ud-Din , Abdullah Ali Faruq , Abu Raihan Mostofa Kamal and Prof. Dr. Abdul Mottalib
[26] "A Security Adaptive Protocol Suite: Ranked Neighbor Discovery (RND) and Security Adaptive AODV (SA-AODV)" 5th International Conference on Electrical and Computer Engineering ICECE 2008, 20-22 December 2008, Dhaka, Bangladesh.