Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 3): pp.4163-4172
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.03.430

# Aodv Routing System For Manets Security And Efficiency

**Neha Garg** Department of Computer Science & Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002 nehagarg@geu.ac.in

**Richa Gupta** Department of Computer Science & Engineering Graphic Era Hill University, Dehradun, Uttarakhand India, 248002 richagupta@gehu.ac.in

**ABSTRACT**

There are a variety of applications for networks. Its widespread use was a driving force behind the development of mobile ad-hoc networks (MANETs). A mobile ad-hoc network is a decentralised wireless technology that generates a network that can adapt quickly to new circumstances. MANET is a growing dynamic network that is also sometimes referred to as mobile mesh network. This is because of the dynamic aspect of MANET, which includes its changing topology as well as the fact that it is wireless. Due to the fact that MANETs are collaborative and open systems, as well as the limited availability of assets, they present a number of different sorts of security concerns. When compared to more conventional networks, the routing is more complicated because there is no central coordinator to oversee it. The ad hoc on demand distance vector, often known as AODV, is the most popular and commonly used routing protocol in mobile ad hoc networks. This is because it possesses several qualities that are helpful to the network. When a particular host or node fails, it will send a message to the source about this failure, which will cause the performance to degrade. The performance of the AODV Reactive routing protocol is presented in this work, coupled with an examination of the many attacks that are possible to execute against AODV. In addition to this, it provides a description of two layer signature security techniques, one of which is a secure hash algorithm designed to enhance the typical performance of AODV. The AODV protocol is extended here, which contains a secure cryptographic hash and a digital signature method. The goal of this modification is to further improve the security of the protocol while maintaining the network's performance. Using NS2 simulator, which is a discrete event-driven simulator, we have successfully implemented the recommended approach. This helps to enhance things like performance and security, which are both important considerations.

## I. INTRODUCTION

In numerous contexts, networks play an important role. Mobile ad hoc networks have arisen as a direct result of its widespread adoption (MANETs). A mobile Ad-hoc network is a

dynamic, decentralized, wireless system. MANET is a growing dynamic network that is frequently referred to as a mobile mesh network due to its dynamic nature and dynamic topology and wireless nature. Due to its open, collaborative design and limited resources, MANETs present a number of unique security challenges. The lack of a centralized coordinator increases the complexity of the routing compared to more conventional networks. The ad hoc on demand distance vector (AODV) routing protocol is the most often utilised option in a mobile ad hoc network. When a host or node fails, a message is sent back to the source, causing a drop in performance. In this research, we analyse the potential vulnerabilities of the AODV Reactive Routing Protocol and show its performance metrics. It also details two-layer signature security approaches, such as the secure hash algorithm, that aim to boost regular AODV's efficiency. By adding a safe hash algorithm and digital signature system, this study extends the AODV protocol to make it more secure and efficient in networks. The proposed method is realized with the help of the discrete event-driven NS2 simulator. This aids in enhancing things like performance and safety.

Broadly speaking, wireless networks are either infrastructure-based or ad hoc. In ad hoc networks , nodes are free to move about and act as routers for other nodes if they are not within radio range of the source or destination nodes directly. Routing protocols are critical to the quality of service and the performance of ad hoc networks because of the networks' inherent fluidity. To put it simply, a MANET is a collection of mobile computing devices such as laptops, PDAs, cell phones, and other similar wireless devices that can communicate with one another.

Some of the challenges and features of MANET are as follows.

- ✓ In dynamic topologies, node mobility is unrestricted. As a result, the topology of the network may undergo sudden and erratic shifts at any time.
- ✓ Variable bandwidth links: Wireless connections typically have far lesser capacity than their hardwired counterparts. In addition, the examined throughput of wireless communications is typically substantially lower than the maximum transmission rate of a radio due to the impacts of multiple accesses, noise, fading, and the occurrence of interfering situations.
- ✓ Limited energy supply: MANET nodes may use finite resources like batteries or solar panels. Conserving energy is a significant priority while designing these nodes.
- ✓ Safety: Physical security concerns against mobile wireless networks are often higher than those against fixed-cable networks. Spoofing, eavesdropping, and denial-of-service assaults are just some of the issues that need to be properly examined. Due to its unique characteristics and difficulties, designing a protocol for the mobile Internet necessitates a different set of assumptions and performance issues than those that govern routing within the fixed Internet's fast, semi-static architecture.

## II. LITERATURE SURVEY

Some other articles provide solutions that combine cryptographic methods with trust-based ones. Comparisons across protocols can be found in articles like the one by Liu et al. [1], as well as others like it. The research that Jared Cordasco and Susanne Wetzel have conducted comparing SAODV with TAODV is of the highest quality, and it includes a comparison of the two systems' performance on hardware with restricted resources. Concerning the security of routing, this article discusses cryptography and trust methods [2]. His approach isn't effective, though, because it requires constant, meticulous attention to the nodes in close proximity. Methods based on the reader's trust are presented in previous publications . Taking into account both node trust and route trust metrics, Meka et al.[3] suggested a trust-based solution (called Trust AODV, or TAODV) that isolates malicious nodes, penalises uncooperative nodes, and allows for the best route to the destination to be determined. Another trust-based method will be offered in this work using trust level, which can provide more relevant concepts along the implementation path than earlier works presented. An alternative trusted routing protocol that addresses security and selfishness concerns is proposed in a different article. This protocol, known as the TAODV protocol, is created using a trusted framework and an intrusion detection system (secure protocol). Trust information can be gathered directly from monitoring nodes and added to the routing table in this paradigm. Therefore, this model guarantees a substantial reduction in overhead while also ensuring the dependability of the routing mechanism [4]. Even with its improvements, TAODV is not yet a flawless protocol. The trust level synchronisation option on distinct nodes is not supported when several pathways converge. Tactical On-Demand Distance Vector (TAODV) routing protocol [5] is an attempt by certain academics to boost MANET performance. The new technique drastically lessens network traffic while while boosting network performance. This procedure is carried out competently, although it has room for improvement in terms of speed and efficiency.

## III. PROPOSED METHODOLOGY

To protect AODV communications, a secret-key encryption technique is proposed here. Each field in an AODV message is encrypted separately, and the signature is then calculated using the proper encryption algorithm. Together with the AODV messages, it will also transmit a signature that was calculated using a secret key. Using cryptographic methods to enforce mutual trust relationships between wireless nodes is a common method of protecting routing protocols [8].

First, in AODV routing, the signature is generated by the sender node using an encryption technique, and then it is appended to each AODV message. The following processes are reorganised:

To recreate signatures, it uses the hash value produced by the trustworthy Secure Hash Algorithm (SHA) include the message's SHA value as the signature. At this time, the sender uses a private key to generate a new signature and appends it to the message before it is sent to the destination node.

After that, each intermediate node that gets the message performs the following computations to double-check that it's the real deal

To determine whether or not to forward a message to the following node in the chain, intermediary nodes utilize the concatenation signature to check the freshly produced signature. However, before rebroadcasting a message, it will verify the index of the next node to see if it is the destination.

Third, the receiving node will compare the appended special signature with the key if the index value indicates that it is the destination node, and if the two signatures match, the secret key will be used to calculate the signature for further security.

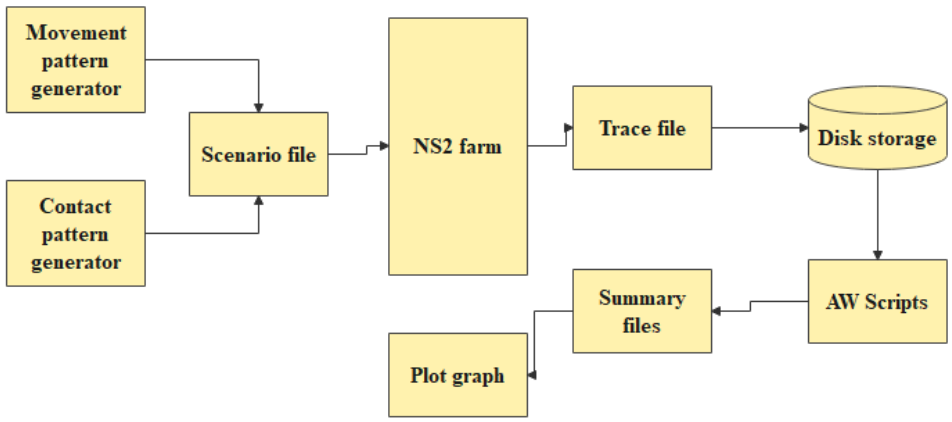


**Fig 1: Proposed block diagram architecture**

Nodes in between the source and the destination use the first signature. Firstly, the sender generates two signatures and appends them to the initial AODV packet as illustrated in Figure 1. If the first signature matches, the intermediate node accepts the packet and sends it on to the next node. When a packet reaches its destination node, a second signature is checked to ensure that it was transmitted by an authorized sender and has not been tampered with in transit. The packets will travel safely from their origin to their final destination.When a node or connection fails, it is recommended that data packets be sent onwards from the previous node they were received at.

Here are some of the changes that have been made:

- ✓ As a result, both connection speeds and throughput improved.
- ✓ The main benefit is that it requires less effort and time.
- ✓ Consequently, there will be no gridlock.
- ✓ Receiving nodes won't hold back to wait for sending nodes.
- ✓ To strengthen security, there is no longer a need to repeatedly apply the same security steps, procedures, and functions to the same data packet.
- ✓ Since AODV's topology is always evolving, it's beneficial to submit data as soon as possible before making any adjustments.

The suggested system decreases end-to-end time in high mobility instances and is highly adaptable, scalable, and efficient. The safety of routing protocols is another area where this plan excels. The AODV routing protocol can be simulated in NS2 . Because NS2 has helpful documentation and researchers can easily reach out to each other for assistance. What's more, NS2 has been utilized in numerous relevant research articles, all of which encourage using it to replicate MANET protocols, which is where my own expertise lies. Therefore, NS2 is the greatest option for this goal. There are a number of methods used to boost performance and safeguards. The NS2 simulator was updated using that way to boost performance.

The proposed methodology made advantage of the aforementioned simulation procedures. The table below displays the various implementation-related configuration values.

All simulation tests are designed and run on a computer with an Intel(R) Core(TM) 2 Duo(TM) 1.83 GHz processor, Ubuntu(R) 12.0.4 operating system, 2 GB RAM, and the network simulators NS2 edition NS- 2.34. There are a number of factors that led to the selection of this particular simulation software. Fifty mobile nodes are spread out over a 1500 metre by 300 metre area in the virtual network. The antenna configuration used for the Two Ray Ground propagation mode has 32 Omni Antennas. IEEE802.11 is utilised for the MAC layer of communication. The full duration of the simulation is 300 seconds. All simulations were run using the parameters listed above.

## IV. RESULTS AND DISCUSSION

A successful deployment of the proposed secure AODV led to two noteworthy outcomes. The first describes a scenario in which an attack is not being launched, whereas the second describes an actual attack. The simulation was run three times, resulting in three unique trace files. Three separate trace files were evaluated with AWK scripts.

### a) Packet delivery rate

It is the comparison between the number of packets sent and received by the traffic analysis generator. Packets received/packets sent are the indicators. Loss of packets, due to things

like network problems or uncooperative behaviour, has a direct impact on the packet delivery ratio.

The preceding graph suggests that there is little to no change in delivery rate after adding security, suggesting that the suggested AODV incurs only a small performance hit from the lack of an attack. However, in the case of the suggested AODV with attack, the PDF drops considerably as a result of the assault.

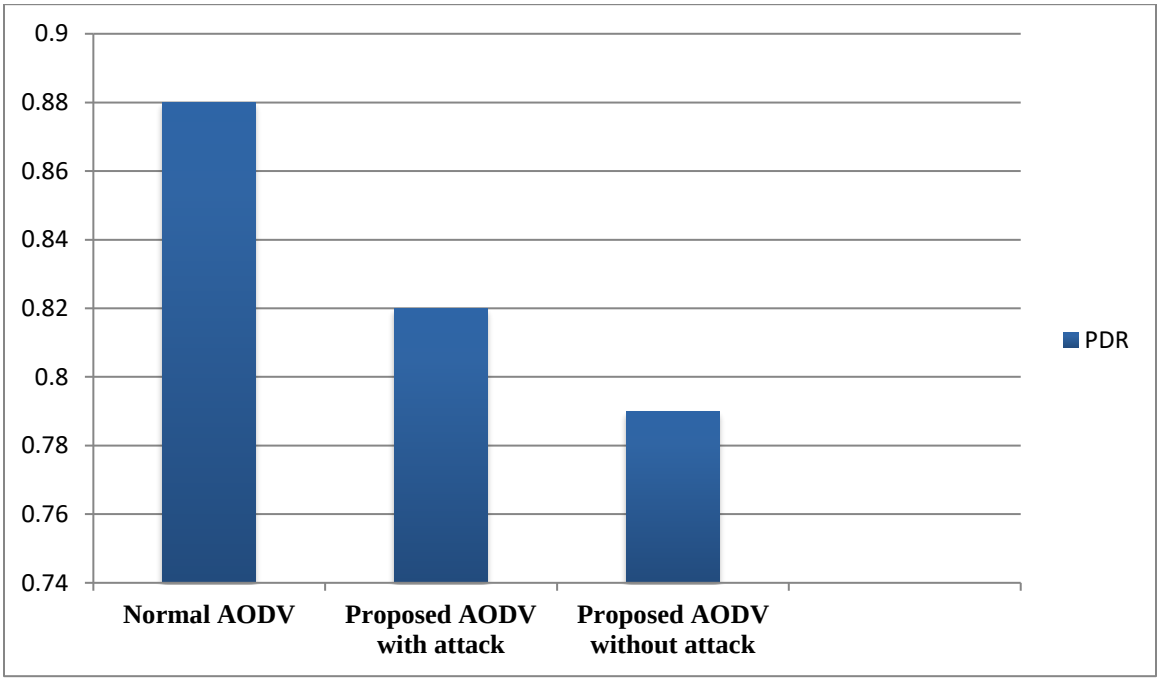


Fig 2: Packet delivery ratio

### b) Average end to end delay

How long it takes for a data packet to travel from its point of origin to its final destination is known as its end-to-end delay. The Normal AODV, the Proposed AODV without attack, and the Proposed AODV with attack are all being tested in this experiment to see which one has the lowest average end-to-end delay.

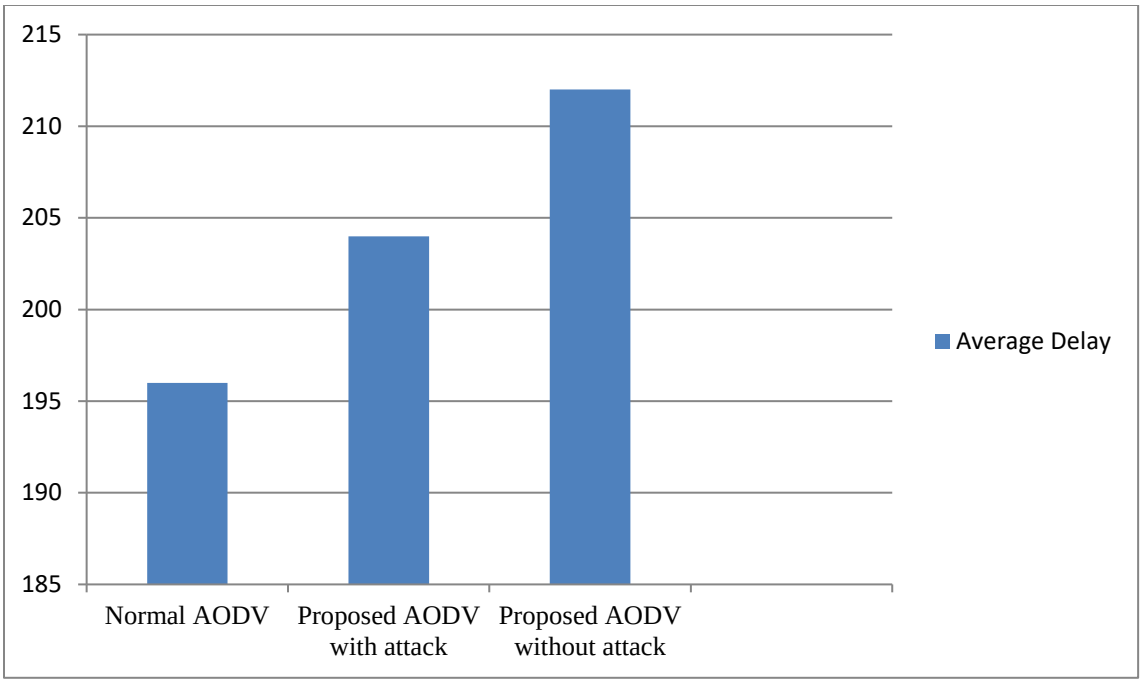


**Fig 3: Average end to end delay**

As can be seen in the figure above, the end-to-end delay does not change significantly after adding security, even in the situation of the planned AODV where there is no assault. The suggested AODV with attack, on the other hand, has been shown to significantly reduce end-to-end delay.

### c) Throughput

As a network metric, it indicates how much of the available bandwidth is actually being put to good use. chooses an endpoint before the simulation begins; this will tell you if or not packets of data made it to their destinations successfully.

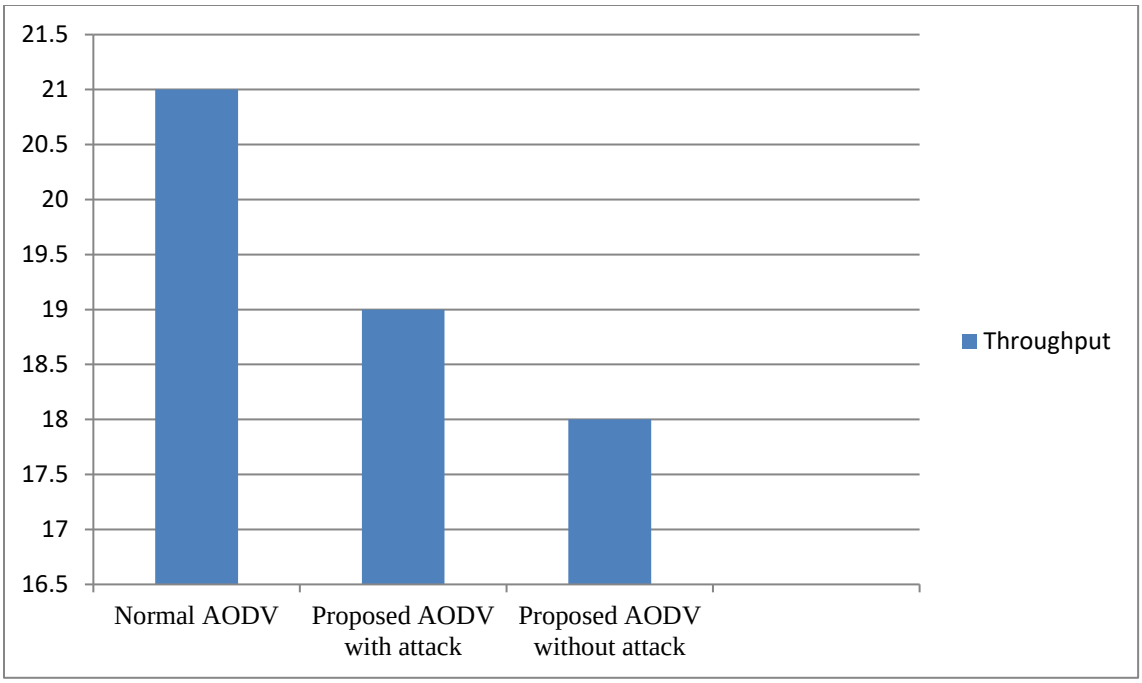


**Fig 4: Throughput**

It can be seen in the below figure that even after adding security, there is not much of a difference in throughput for the proposed AODV, even in the absence of an attack. The planned AODV under attack experiences a significant drop in throughput.

### d) Jitter

Jitter is a method of randomizing the timing at which packets are transmitted by nodes in a MANET to avoid them from transmitting at the same time while yet maintaining the MANET feature of maximum node autonomy. The Normal AODV, the Proposed AODV without an attacker, and the Proposed AODV with an attacker have all had their Jitter measured in this experiment.

In the following chart, we can see that there is little difference in jitter measurement between the three different procedures.

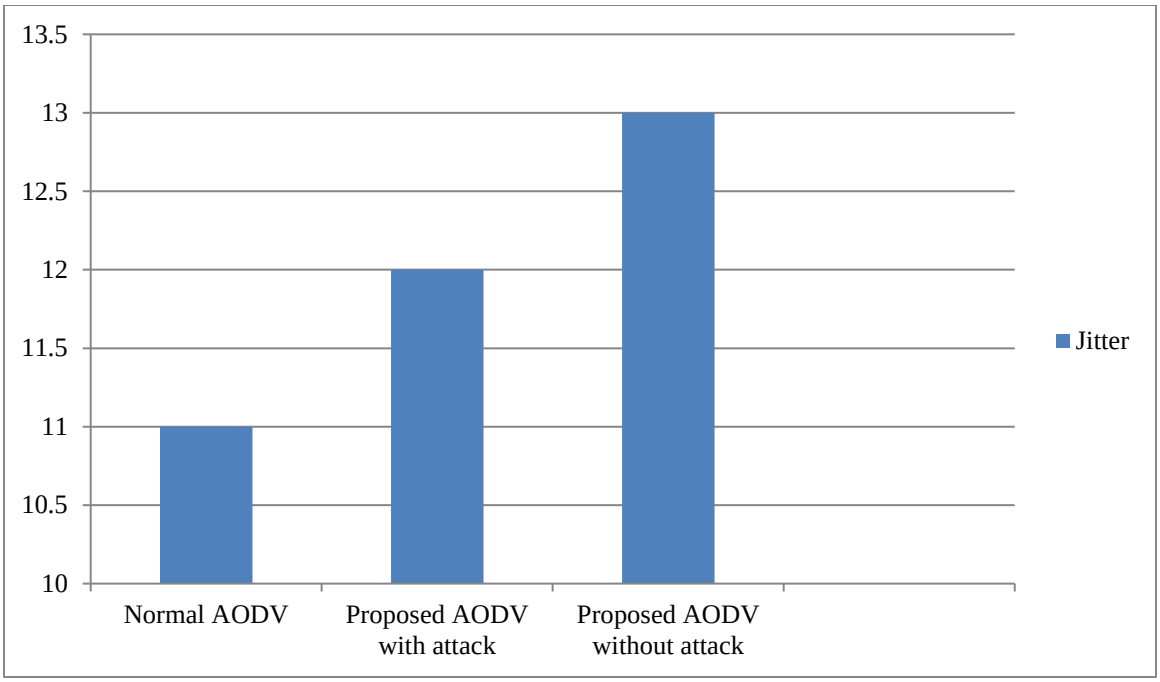


**Fig 5: Jitter comparison**

## V. CONCLUSION

The area of MANETs is undergoing a great deal of development at the moment. Although there are a lot of difficult goals that must be achieved, it is expected that such systems will see broad and extensive use in the coming years. The biggest difficulty here is maintaining safety. The topic of mobile ad hoc network security has lately acquired traction among academics. Security leaks can be a hindrance to basic network operations in ad hoc networks because to their open nature and the lack of underlying infrastructure, therefore countermeasures should be built into the network's functionality from the start.

For MANETs, security solutions must work around constraints such as low power and slow processing speeds. The field of MANET routing protocols uses encryption algorithms, however there has been no prior published work on identifying and protecting against hostile and unauthenticated nodes simultaneously.

This paper provides an overview of the several kinds of routing protocols used in MANETs, as well as a discussion of the pros and cons of each, and a study of the existing proactive, reactive, and secured MANET routing protocols. Then, we dove into the various methods by which MANET routing protocols might be compromised. After that, the basics and operation of basic AODV are covered, along with possible attacks on it.

The next suggestion is to improve the AODV protocol's safety and speed. For the safety of the MANET's AODV routing protocol, it is described here. This solution is more easily scalable

and computationally simpler because it satisfies all security needs without relying on a centralized certification authority or key management mechanism. Since it generates negligible extra work in the form of calculations, it considerably reduces the load on individual nodes and hence their energy needs. Furthermore, numerous explanations were provided regarding why the NS-2 simulations programmed was used to carry out all the studies.

For the future, we will suggest the following concepts that can be incorporated into the suggested design. Routing protocols in MANET, such as DSR, DSDV, TORA, etc., will all benefit from the same type of security integration and implementation. Wireless sensor networks will also be protected by the same type of security mechanism. Further, optimization between protocol layers can help boost the performance of other protocols as well.