2nd International Conference on Current Research Trends in Engineering and Technology
2018 IJSRSET | Volume 4 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Security Enhancement with Performance using Double Digest Mechanism in AODV for MANETs

Pratiksha Raval[*1], Vikram Solanki[2], Nimit Modi[3], Pritesh Patel[4], Kaushal Patel[5], Dipak Agrawal[6]

[1-5]Computer Engineering, Sigma Institute of Engineering, Vadodara, Gujarat, India
[6]Computer Engineering, Sigma Institute of Engineering, Vadodara, Gujarat, India

ABSTRACT

Mobile Ad hoc Network's because of maliciousness that intentionally disrupts the network by using variety of attacks and due to routing protocols (e.g. AODV), which were already developed without considering security features to prevent the various kinds of attacks. And also there is infrastructure less environment, and having open peer-to-peer architecture, shared wireless medium and dynamic topology, MANETs are frequently established in insecure environments like disaster sites and military applications. The AODV routing protocol was initially developed without considering security in mind. So it is not able to defend against any kind of security attack. But there are many security schemes available that make AODV secure. However, by doing more research in this area, one major flaw in any of the existing secure routing protocols was discovered. That is security schemes that are available consume more processing power and required complex key-management system. In this work I am going to present a novel security scheme which integrates dual digest mechanism with symmetric key distribution security scheme to protect the AODV routing protocol that is capable of defending itself against both malicious and unauthenticated nodes. The proposed security scheme will also be simulated in the Network Simulator 2.

Keywords : Mobile Ad-hoc networks, Reactive routing protocol, Throughput, Route discovery, SHA algorithm, NS2, AODV, Symmetric Key Distributor, Dual Digest.

I. INTRODUCTION

A. Ad-hoc networks

Wireless networks [1] can be broadly classified into infrastructure based wireless networks or ad-hoc networks. In ad-hoc networks [2], the nodes are mobile and routing between source and destination node is achieved by intermediate nodes acting as routers if not in radio range. As ad-hoc networks are highly dynamic, routing protocols play a crucial role to achieved quality of service and performance. Basically MANET is defined as a group of wireless computing devices like Laptop, Personal digital assistant (PDA), cell phones or other similar devices [4].

Mobile Ad Hoc Networks challenges and features are:

1) Dynamic topologies:

Nodes are allowed to move randomly. Thus, the network topology may change randomly and rapidly at unpredictable times [3].

2) Bandwidth - constrained, variable capacity links:

Wireless links have significantly lower capacity than their hardwired counterparts. In addition the examined throughput of wireless communications, because of the effects of multiple access, noise, fading and instance of

interfering conditions, is often much less than a radio's maximum transmission rate [5].

3) Energy-constrained operation:
All the nodes in MANET may depend on batteries and other exhaustible means for their energy. For these nodes, the most important design criteria are energy conservation [5].

4) Security:
Mobile wireless networks are generally more likely to physical security threats than fixed-cable networks. The various problems like spoofing, eavesdropping, and denial-of- service attacks should be carefully considered these characteristics and challenges make a set of necessary assumptions and performance issues for protocol design which extend beyond those guiding the design of routing within the high speed, semi static topology of the fixed Internet.

B. Routing protocols
In mobile ad-hoc networks routing protocols are broadly classified into Reactive routing protocol, Proactive routing protocol and Hybrid protocols. Routing protocols in MANET are used to discover different path between nodes. They do not use any access points for connecting each node to other node in network. They generally divided into three categories: it will describe the comparison of these three protocols. These comparisons were based on parameters like number of input, time analysis, rate of sending data for packet delivery ratio (PDR), end to end delay and load [4].

In proactive routing each node maintains a table containing routing related information. Any node wants to transmit data can start transmitting data using routes already present in the routing table enabling data transmission. proactive routing protocol includes destination sequence distance vector (DSDV) routing protocol as well as many other routing protocol like optimized link state routing protocol (OLSR), wireless routing protocol (WRP). Here the advantage of proactive protocols updates its routing table data irrespective of data traffic [4].

Reactive protocols update routing information only when route is required, these protocols reduce the overhead in mobile networks. Some of the famous ad-hoc routing protocols falling in this type are Dynamic Source Routing (DSR), Ad-hoc On Demand Distance Vector (AODV) routing and Temporarily Ordered Routing Protocols (TORA) [4].

C. AODV Reactive routing protocol
AODV is a remodelling of destination sequence distance vector (DSDV) protocol used in wireless mobile networks. This solves the disadvantages of DSDV by implementing a sequence number. Not like DSR [9] which carries the entire route from source to destination in the packet, the nodes in AODV carry out the next hop information corresponding to each data flow. Being a Reactive protocol route is discovered as when needed and maintained as long as they required. Hybrid protocols have well combination form of both reactive and proactive routing protocols methods [4].

D. Various Possible Attacks in MANET:
Many possible attacks can compromise the security of AODV in mobile ad hoc network

Internal attacks:
In this type, the attacker acts as one of the nodes and gains direct access to the network either by impersonation or by compromising a proper node and using it to do its malicious activities.

External attacks:

In this type, the attacker attacks from outside the network, due to congestion in the network traffic by propagating non meaningful messages, thereby disturb the entire communication of the network.

1) Impersonation:

This type of attack is one of the most severe attacks. In this type the attacker can act as an innocent node and join the network. Same way, when several such nodes join the network, they gain the full control of the network and conduct malicious behavior. They spread fake routing information and they also gain access to confidential information. A network is vulnerable to such attacks if it does not employ a proper authentication mechanism [9].

2) Eavesdropping:

In this type of attack the goal of the attacker is to get some private information while it is being transmitted from one node to the other. This attack is very hard to find out and the secret information like private key, public key, password etc. of the nodes can get compromised due to this attack [9].

3) Denial of Service:

The main goal of this type of attack is to make sure that a specific node is not available for service. The entire service of the network might be compromised due to this attack [9].

4) Wormhole attack:

In this type of attack the opponent connects two distant parts of the network and underpass messages received in one part of the network to the other. In this type a lower latency link is used to pass the messages [9].

5) Black hole attack:

In this type of attack the opponent traps the traffic of the network close to a compromised node and thus a black hole is created with the opponent at main centre. Basically the attacker offers an attractive path to the neighbouring nodes. This attack can also be coupled with other attacks like dropping packets, denial of service, replay of knowledge, selective forwarding [9].

6) Sybil attack:

In this type of an attack, a particular node tries to have several different fake identities. This way helps the malicious node to gain more and more information about the network. The validness of fault tolerant schemes like distributed storage; multipath routing topology maintenance etc. has a great decrease [6], [9].

II. METHODS AND MATERIAL

AODV [7] is based on distance vector routing. When security is applied to it, the performance of the network degrades. So the problem solved here is to incept security in such a manner that the performance degradation is as low as possible.

Here the considered problems are:

- If nodes or links fails then error message is sent back to the source this will activate the source nodes to resend the data back to destination and this will take too much time to perform the procedure again.
- It is time consuming.
- Traffic congestion increases as same packet is send again and again.
- The effect of traffic congestion will pay impact on the Performance/Throughput of AODV system due to resending of same packet will cause other nodes waited to send data. The

security of AODV will be based on one-way hash, two-way hash and digital signature.

All the three security procedure consists of several steps. It required many inbuilt functions. This general Procedure needs to be proceeding before sending and receiving the packet. Now if nodes or links fails, so all the process inbuilt functions needs to be conducted again to same packet.

Here an encryption algorithm with Secret key is proposed to secure AODV messages. This mechanism calculates signature using appropriate encryption algorithm for all the fields of an AODV message. It also calculates signature with secret key and then both signatures will be transmitted along with the AODV messages. Cryptographic mechanisms are commonly used to protect routing protocols by enforcing mutual trust relationships among the wireless nodes [8].

1) In AODV routing, sender node produces the signature with an encryption algorithm and concatenates it with each of the AODV messages. It reforms the below operations:

- It make use of secure hash algorithm (SHA) [10] value to regenerate signature.
- Assign a signature SHA value with the message format.
- Now for specially destination node sender make use of a secret key to produce another signature and generate the same and also concatenates it with message.

2) Subsequently, every time an intermediate node receives the message, it calculates the following calculations to recheck the genuine message:

It makes use of the concatenated signature to compare the newly generated signature by intermediate node; if it matches then node will carry forward the message to the next node. But before re-broadcasting a message it will check the index of upcoming node to check whether it is destination or not.

3) Finally if receiving node matches the value of index and find it is destination node then, it will calculate the signature with using secret key for more security purpose and compare it with concatenated special signature with key.

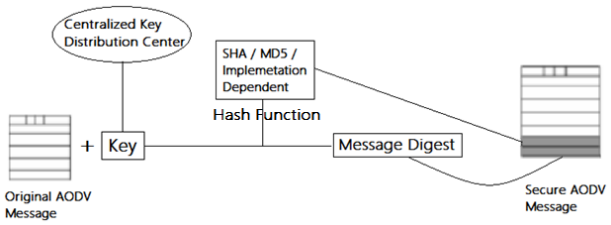

Figure 1: Dual Digest Security Mechanism Scenario 1

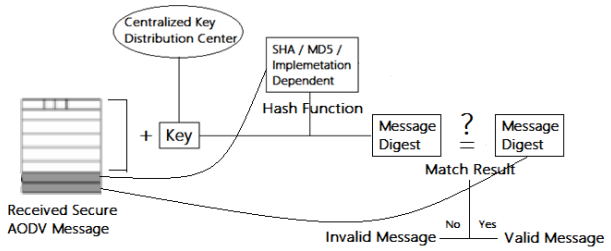

Figure 2: Dual Digest Security Mechanism Scenario 2

First Signature is used for intermediate nodes while second signature is for destination. As shown in the figure 1, sender first generate two signatures, and it concatenates those signature in the original AODV packet, intermediate nodes will verify the packet using first signature, if first signature will match it will accept the packet and forward it to the next node. When packet will arrive to the destination node it will check for second signature and verify its authenticity that

packet was sent by legal sender and it is not being modified. In this way, packets will transfer from source to destination securely.

Here it has been proposed that, send the data packet from the last nodes it received when particular node or link fails instead of sending it back.

Improvements done are:

- Network performance and throughput both increased.
- It is less time consuming.
- Traffic congestion will not occur.
- Other nodes will not be going to wait for nodes that are sending.
- No need to apply security steps, procedure and functions again and again on the same data packet and hence security increase.
- As AODV is dynamic in nature therefore its topology changes quickly so it helps to send the data quickly before changing its topology.

The proposed scheme will be highly flexible, easily expanded and efficient and mainly reduces end to end delay in high mobility cases. Also this scheme will improve security for routing protocol. For implementation, NS2 simulator [11] is used for AODV routing protocol. As NS2's documentation is good and easy to get support from many researchers using it. Additionally, many papers related to my field of research have used it and they recommend using NS2 to simulate MANET protocols. Thus NS2 provide the best solution to the said purpose. Many factors have been applied for improving performance along with security. That methodology was applied in NS2 simulator to improve the performance factor.

The above simulation action were used in the propose methodology. The different configuration values which were used for implementation are given below in the table.

TABLE 1: SIMULATION PARAMETER TABLE

Parameter	Value
MANET Area	1500*300 sq.m.
Total number of nodes	50
Node speed	0 up to 20 m/s
Application	Constant bit rate
Number of generated packets	10000 packets per CBR
Size of packets	512 bytes
Simulation time	300 sec

III. RESULTS AND DISCUSSION

After implementation of successful proposed secure AODV, There were two different situations to be highly regarded. First is without attack situation and second is with attack situation. Total three times the simulation was ran and three different trace files were generated. With the use of AWK scripts the three different trace files were analysed.

A. Data Traffic (CBR) Comparison

In order to measure packet delivery fraction, it is necessary to count the total number of sent, received and routed packets. Following graph shows the total number of sent, received and routed packets for simulation environment.

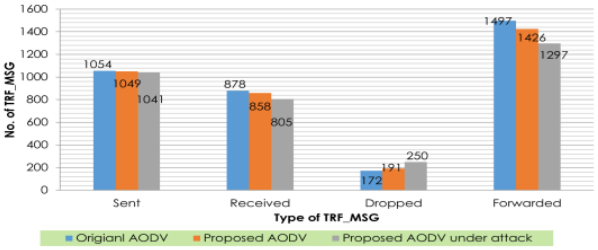

Figure 3: Data Traffic (CBR) Comparison

B. Data Traffic (CBR) Delivery Rate

Delivery rate for each protocol can be counted by calculating Received/Sent Packets. Below graph shows delivery rate:

From the below figure it can be concluded that in case of proposed AODV without attack the delivery rate is decreasing marginally, which is a good indication. It shows that there is not much difference in delivery rate even after adding the security. While in case of proposed AODV with attack the delivery rate decreasing noticeably due to the attack. Than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader.

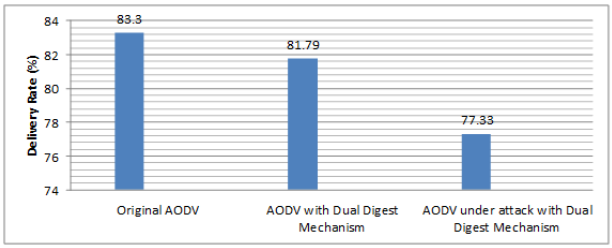

Figure 4: Data Traffic (CBR) Delivery Rate

C. Packet Delivery Fraction (PDF)

It is the ratio of packets delivered to that produced by the traffic analyses generator. It is shown by received packets/sent packets. The packet delivery ratio is directly influenced by loss of packets, which may be caused by general network faults or uncooperative behaviour.

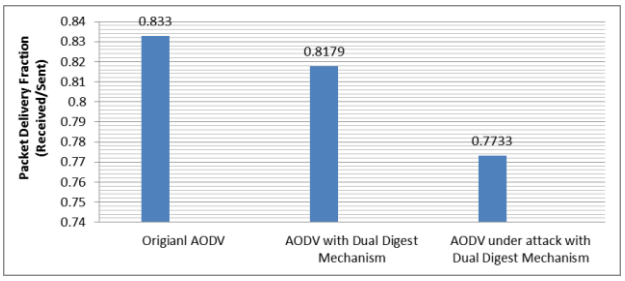

Figure 5: Packet Delivery Fraction (PDF)

D. Average End to End Delay

The average end-to-end delay of data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination. In this experiment, the average end-to-end delay is being measured for the Normal AODV, Proposed AODV without attack and Proposed AODV with attack.

From the below figure it can be concluded that in case of proposed AODV without attack the E2E delay is increasing marginally, which is good indication of showing there is not much difference in end-to-end delay even after adding the security. While in case of proposed AODV with attack the end-to-end delay is decreasing noticeably due to the attack.

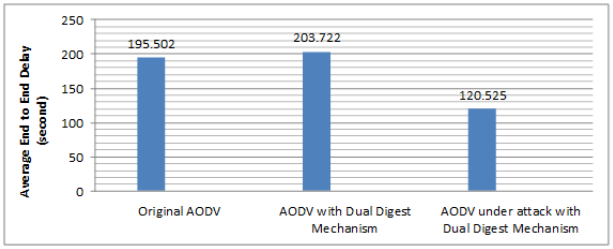

Figure 6: Average End to End Delay

E. Average Throughput

It is one of the dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation i.e., useful information whether or not data packets correctly delivered to the destinations.

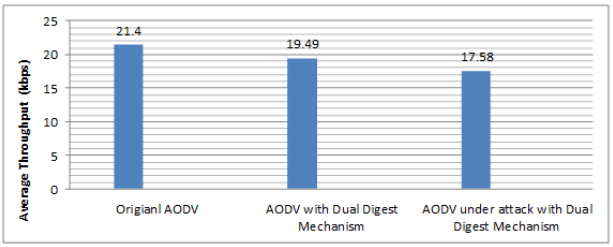

Figure 7: Average Throughput

From the below figure it can be concluded that in case of proposed AODV without attack the throughput is decreasing marginally, which is good indication of showing there is not much difference in throughput even after adding the security. In case of proposed AODV with attack, throughput decreasing noticeably due to the attack

IV. CONCLUSION

There are many changes appear in the field of MANETs. While there are many challenging task that need to be met, it is likely that such networks will observe widespread and extensive use within next few years. Here the main challenge is security. Mobile ad-hoc networks' security issue has recently gained momentum in the research community. Because of the open nature of ad-hoc networks and their inherent lack of infrastructure, security disclosures can be an impediment to basic nature operations and countermeasures should be included in the network functions from the early stages of their design.

In future, we will further propose some ideas that can be integrated to the proposed scheme and they are presented as follows: The same kind of secure mechanism will be integrated and implemented to secure other routing protocols of MANET like DSR, DSDV, TORA etc. the same kind of secure mechanism will be designed to secure wireless sensor networks also. Even the performance factor improvement of other protocols by optimization between different layers is in line up.

V. REFERENCES

[1] S. Doshi, T. X. Brown, Minimum Energy Routing schemes in Wireless Ad hoc networks, IEEE INFOCOM 2002

[2] Ram Ramanathan and Jason Redi, "A brief overview of Ad-hoc Networks: Challenges and Directions", IEEE Communications Magazine May 2002, pp. 20-22

[3] Mitigating Black Hole Attacks in AODVISSN 0975-3303Mapana J Sci, 11, 4(2012), 65-76 Routing Protocol Using Dynamic Graph

[4] Brijesh Soni, Biplab Kumar Sarkar, Arjun Rajput, "Improvising the Ad hoc on Demand Distance Vector Routing Protocol When Nodes or Links Fails," *in Proceedings of All India Seminar on Biomedical Engineering 2012 (AISOBE 2012) © Springer India*

[5] International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011 DOI : 10.5121/ijnsa.2011.3518 229Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism

[6] A Study of Secure Routing in MANET: various attacks on AODV in MANET.

[7] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance Vector (aodv) routing," *IETF RFC 3591*, 2003.

[8] A. A. Pirzada and C. McDonald, "Establishing trust in pure ad-hoc networks," *Proceedings of the 27th Australasian Computer Science Conference (ACSC)*, vol. 26, no. 1, pp. 47–54, 2004.

[9] Weichao Wang, Yi Lu, Bharat Bhargava, "On Security Study of Two Distance Vector Routing Protocols for Mobile Adhoc

Networks", (IEEE) 2003, 0-7695-1893-1/03

[10] Eastlake D, Jones P (2001) US Secure Hash Algorithm (SHA1). RFC 3174.

[11] E. Altman and T. Jimenez, Lecture Notes on NS Simulator for Beginners, December 03, 2003.

[12] The Network Simulator – NS2. (http://www.isi.edu/nsnam/ns/index.html).