IJSRD - International Journal for Scientific Research & Development| Vol. 3, Issue 04, 2015 | ISSN (online): 2321-0613

Security Enhancement over AODV by Establishing Symmetric Key Cryptography

Amruta Upadhyay[1] Vanraj.B.Vaghela[2]
[1]P.G Student [2]Principal
[1]Department of Electronics and Communication Engineering
[1]Sankalchand Patel college of Engineering, Visnagar, Gujarat Technological University.University of Gujarat (India) [2]Jashodaba Polytechnic Institute, Sidhpur, Gujarat Technological University, University of Gujarat (India)

Abstract— Communication takes place by routing protocols in efficient and effective manner in wireless network. Efficient protocols are used to forward data packets without much packet loss. MANET (Mobile Ad hoc Network) because of maliciousness that intentionally disrupts the network by using variety of attacks and due to routing protocols e.g. AODV (Adhoc On demand Distance Vector), which were already developed without considering proper security features to prevent the various kinds of attacks. 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. 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 we are going to present a novel security scheme which integrates Key Distribution & Authentication Server and Secure Hash Function mechanism to protect the AODV routing protocol that is capable of defending itself against both malicious and unauthenticated nodes. The proposed security scheme will be simulated in the Network Simulator 2.

Key words: Mobile Ad Hoc Network security, AODV Routing Protocol, Public Key Cryptography, SHA-1, NS-2.34

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a remote system the nodes that are in radio range of one another can specifically convey, though others needs the guide of intermediate nodes to route their packets. These systems are completely disseminated, and can work at wherever without the assistance of any framework. This property makes these systems profoundly adaptable and robust. The dynamic change in MANET topology makes routing as a testing task, as the current way is rendered wasteful and infeasible. The real issues for mobile ad hoc systems are medium access control (MAC), routing, security and nature of administration provisioning. The paper addresses the routing issue in a mobile specially appointed system without considering alternate issues,

i.e., access control and security. Directing in MANET implies the guided stream of information from source to destination boosting the system execution. The attributes of these systems are outlined as takes after:

– Wireless Communication
– No centralized controller.
– Dynamic topology.
– Frequent routing updates.
– Nodes can perform the parts of both hosts and routers.
– Intrinsic shared trust.

Some of the uses of MANETs are

– Disaster alleviation operations.
– Defence Development.
– Urgent Business gatherings.
– Mine site operations.

System Simulator (NS-2) is an event driven, object situated system simulating device, all that much utilized by the specialists, teachers and understudies. Simulation is the procedure of making a model with its conduct. There are various system simulating tools accessible, for example, NS-2, OPNET, GloMoSim, QualNet, and so forth. NS-2 is the beats among the various tools. The Routing conventions of MANET, for example, DSDV, DSR, AODV is actualized utilizing NS-2 and it's accessible as free open source programs. In this paper, AODV convention is considered and its system execution is enhanced with security.

The rest of the paper is organized as follows: Section II gives an overview of Routing Protocols of MANET with security The rest of the paper is organized as follows: Section II gives an overview of Routing Protocols of MANET with security and it's Security issues and Section III describes the Reactive Routing Protocol AODV, Section IV discusses the proposed topology used for P-AODV, Section V describes NS-2 implementation of P-AODV, section VI discusses about simulation results and analysis and finally section VII discusses about conclusion derived from the implemented results.

II. ROUTING IN MANET WITH SECURITY

Routing protocols for Mobile Ad Hoc Networks can be broadly divided into two distinct categories, namely proactive (table-driven) routing protocols and reactive (on-demand) routing protocols.

A. *Proactive Routing Protocols:*

Each node maintains up-to-date routing information to every other node in the network. Routing information is kept in a number of routing tables and updates to these tables are periodically transmitted throughout the network to maintain table consistency. Thus, in proactive routing, routes can be quickly established without any delay. However, it requires a significant amount of resources to keep routing information up-to-date.

Reactive or On-demand routing protocols are designed to overcome the increased overhead problem in proactive protocols. Unlike proactive protocols, reactive protocols create a route only when desired. If a node desires to send a message to a destination node for which it does not have a valid route to, it initiates a route discovery to locate the destination node. The process is completed when a source node finds a route to the destination. A route maintenance procedure is implemented to maintain a route until the destination is no longer available or not desired.

Even though reactive protocols overcome increased overhead problem, but they exhibit end-to-end delay since routes are created on demand. Both proactive and reactive routing protocols require persistent cooperative behavior, with intermediate nodes primarily contributing to the route development. Similarly each node, which practically acts like a mobile router, has absolute control over the data that passes through it. In essence, the membership of any ad-hoc networks indisputably calls for sustained depiction of benevolent behavior by all participating nodes [5]. This is often not possible in an open environment; this is the reason why these networks are frequently attacked by malicious nodes, from both inside and outside.

There are two kinds of possible attacks that can be initiated against Mobile Ad Hoc Networks: Passive and Active.

B. Passive Attacks:

In such type of attack, the attacker does not disturb the routing protocol. It only eavesdrops upon the routing traffic and endeavors to extract valuable information like node hierarchy and network topology from it.

C. Active Attacks:

In this, the malicious nodes can disturb the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information, and by impersonating other nodes [2].

Generally cryptographic mechanisms are employed to protect routing protocols by enforcing mutual trust relationships among the wireless nodes. Security in Mobile Ad Hoc Wireless Networks is mainly a dual problem. One is the security of the routing protocols that enable the nodes to communicate with each other and the second is the protection of the data that traverses the network on routes established by the routing protocols. In this paper, we first discuss the traditional AODV routing protocol and the security flaws associated with it. Then we survey some of the secured approaches that have been proposed by different authors in order to secure AODV in a mobile ad hoc environment. We also investigate the experimental comparisons performed on the secured versions of AODV with the traditional AODV.

D. Analysis

There are two approaches to evaluate routing protocols:

- Network Environment Parameters like network size, connectivity, mobility, link capacity etc.
- General Performance Metrics of Routing Protocols like packet delivery ratio, control overhead, hop count, end to end delay, jitter, etc.

In this paper packet delivery ratio, average end to end delay and jitter performance parameters are considered.

III. AODV ROUTING PROTOCOL

AODV protocol allows mobile nodes to quickly obtain routes for new destinations, and it does not require nodes to maintain routes to destinations that are not in active communication. Also, AODV routing permits mobile nodes to respond link breakages and changes in network topology in a timely manner. The main objectives of the protocol is quickly and dynamically adapt to changes of conditions on the network links, for example, due to mobility of nodes the AODV protocol works as a pure on-demand route acquisition system. Control messages used in AODV are:

- Route Request Message (RREQ)
- Route Reply Message (RREP)
- Route Error Message (RERR)
- Route Reply Acknowledgment (RREP-ACK) Message
- HELLO Messages

A. Route Discovery:

When a source node desires to send a message to some destination node, and doesn't have a valid route to the destination, it initiates a path discovery process to locate the other node. It broadcasts a route request (RREQ) control packet to its neighbours, which then forward the request to their neighbours, and so on, either the destination or an intermediate node with a new route to the destination is located.

The AODV protocol utilizes destination sequence numbers to ensure that all routes contain the most recent route information. Each node maintains its own sequence number. During the forwarding process the RREQ intermediate nodes record the address of the neighbour from which the first copy of the broadcast packet is received in their route tables, thereby establishing a reverse path. Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination or the intermediate node responds by unicasting a route reply (RREP) control packet back to the neighbour from which first received the RREQ [6,7].

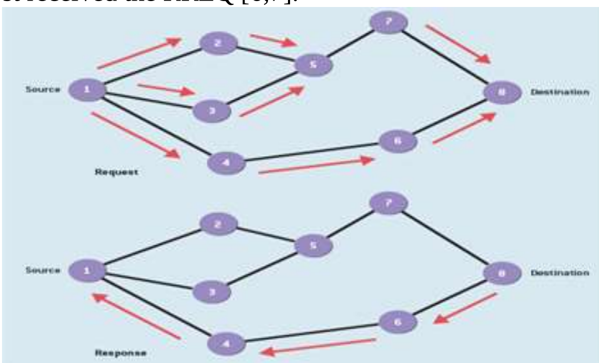

Fig. 1: AODV Route Discovery[8]

B. Route Maintenance:

A route discovered between a source node and destination node is maintained as long as needed by the source node. The destination node or some intermediate node moves, the node upstream of the break initiates Route Error (RERR) message to the affected active upstream neighbors/nodes. Consequently, these nodes propagate the RERR to their predecessor nodes. This process continues until the source node is reached. When RERR is received by the source node, it can either stop sending the data or reinitiate the route discovery mechanism by sending a new RREQ message if the route is still required[9,10].

IV. PROPOSED METHODOLOGY

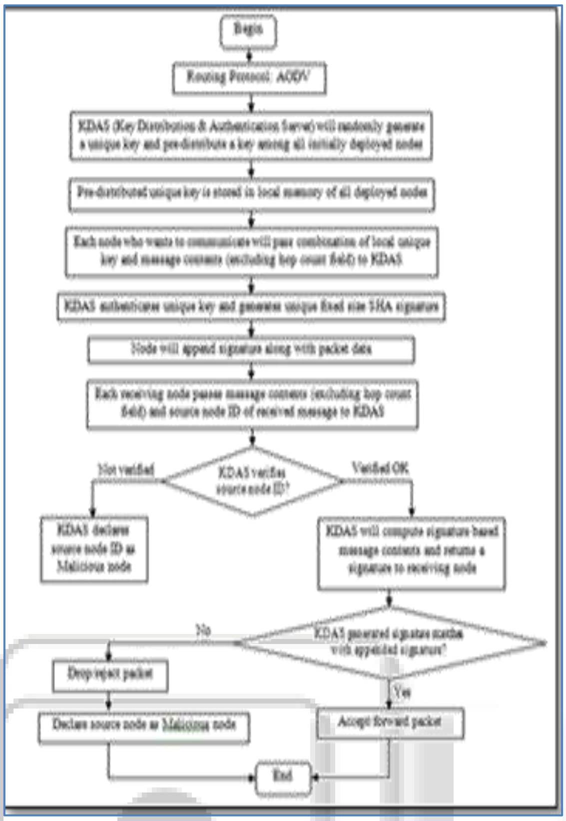

Fig. 2: Proposed Algorithm

V. SIMULATION RESULTS AND ANALYSIS

A. *Simulation:*

We have simulated AODV and our Proposed mitigation scheme and compared them on the basis of certain parameter metrics in Network Simulator- 2.

Parameters	Value
Simulator	NS-2(Version 2.34)
MAC Type	Mac /802.11
Number of mobile nodes	15, 30,45,60 Nodes
Traffic Type	CBR
Traffic connections	TCP
Routing Protocols	AODV

Table 1: Simulation Parameter

B. *Results and Analysis:*

The following metrics are used to analyse the simulation results.

1) B.1 Delivery Rate

Figure B.1 shows the graph between delivery rate and number of attackers among different node scenario. On varying number of attackers, delivery rate gets fluctuate because of nodes' mobility, but it's in the negligible form. Our algorithm mitigates the attacker and gives better result in terms of delivery rate.

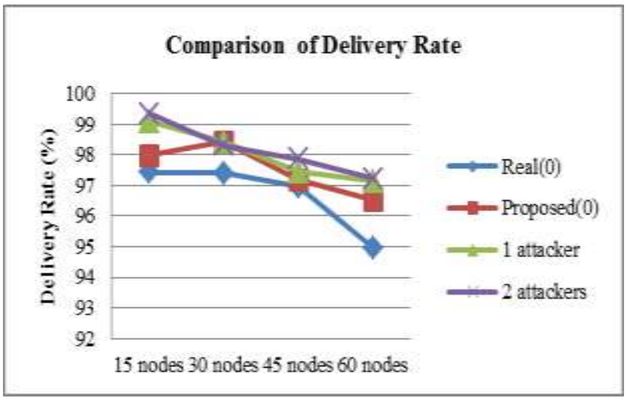

Fig. B.1: Comparison of delivery rate for different node scenario

2) B.2 End to End Delay:

Figure B.2 shows the graph between end to end delay and number of attackers among different node scenario. On varying number of attackers, end to end gets decrease. The reason being, some amount of time is being needed for detection and mitigation of malicious node for security measures. Our algorithm gives better result in terms of performance over end to end delay.

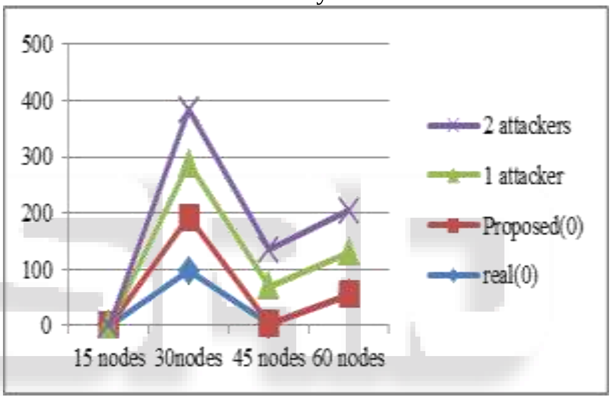

Fig. B.2: Comparison of end to end delay for different node scenario

3) B.3 Jitter:

Figure B.3 shows the graph graph between jitter and number of attackers. On varying Number of attackers, jitter gets decrease. Our algorithm gives better result in terms of jitter.

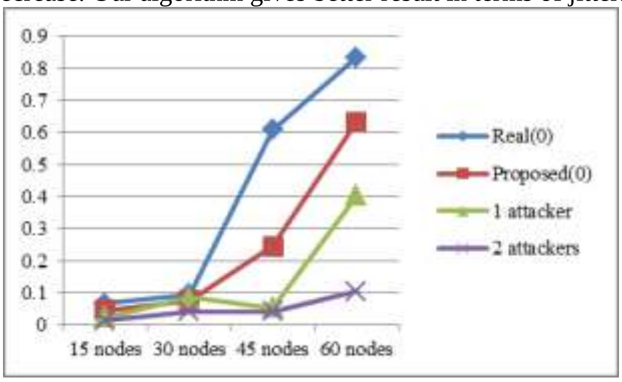

Fig. B.3: Comparison of delivery rate for different node scenario

VI. CONCLUSION

Security of mobile ad hoc networks has recently gained momentum in the research community. Security solutions including limited energy and computational resources. To my knowledge, there is no previously published work on detecting and defending against malicious and unauthenticated nodes together in the field of MANETs' routing protocols using integrating Key Distribution & Authentication Server and Secure Hash Function mechanism in AODV routing protocol to make secure policy to detect and protect against malicious actions by third parties.

By reviewing all the methods Proposed methodology with SHA-1 Function using NS2simulation is considered from them & implemented the Proposed methodology with normalaodv comparison

ACKNOWLEDGMENT

I am beholden to express my obeisance to my mentor Prof. V.B.Vaghela (Principal,Sidhpur) for his hearty support and constant cultivation which is solemnly responsible in bringing our efforts to fruition. I acknowledge my deep sense of gratitude to Prof. Kehul A. Shah (Associate Professor and Head of the Department) for his valuable guidance throughout the work. I express my profound gratitude to Dr. H. B. Patel (I/c Principal) for his outstanding cooperation to provide all the required facilities. I also express my ineptness for the cooperation and technical support provided by my respected professors of Electronics & Communication Department. On personal level, I would like to express my sincere thanks to my family, colleagues and friends for their direct and indirect support and encouragement towards the completion of this work.At last I feel it my bounden duty to express my heartily thankfulness to the entire staff of Electronics & Communication Department for their untiring consistent cooperation.

REFERENCES

[1] Tahira Farid_ and Anitha Prahladachar , Secure Routing with AODV Protocol for Mobile Ad Hoc Networks _University of Windsor, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[2] Patil V.P, " Efficient AODV Routing Protocol for MANET with enhanced packet delivery ratio and minimized end to end delay," in International Journal of Scientific and Research Publications, Volume 2, Issue 8, August 2012

[3] Sandip A. Kahate, Kapil N. Hande2#, " Implementing Authentication Mechanism using Extended Public Key Cryptography in Wireless Network," International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 5, May 2012

[4] Amol Bhosle1 and Yogadhar Pandey2, "Applying Security to Data Using Symmetric Encryption in MANET", International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013)

[5] Binod Vaidya, Dimitrios Makrakis, and Hussein Mouftah, "Provisioning secure on-demand routing protocol in Mobile ad hoc network ",2011 IEEE.

[6] Aruna Sanjay Knodealkar and Dr. Lata R. Ragha,"Security Enabled DSR for Establishing Symmetric Key and Security in MANETs", 2013 IEEE