Secure Route Discovery & Data Transmission on AODV Based MANETs

Kavitha V¹, Sujatha S.G²
kavi.v.10@gmail.com¹, sujatha.sg@cmrit.ac.in²

Abstract

Mobile ad hoc network is a special kind of wireless networks formed without any centralized administration. It is a collection of mobile nodes without having aid of establish infrastructure. In mobile ad hoc network, it is much more vulnerable to attacks than a wired network due to its limited physical security, volatile network topologies, power-constrained operations, intrinsic requirement of mutual trust among all nodes in underlying protocol design and lack of centralized monitoring and management point. The main aim of this work is to provide secure data transmission between the source and destination. To improve the security of such network, technique proposed here is securing routing protocol AODV through the use of Symmetric Encryption algorithm MD5. This secures the data as well as preserves the integrity. The simulation results using the Network Simulator 2 (NS2) demonstrate an improvement in the ratio of packet drop and throughput using our mechanism as compared to the standard AODV protocol.

Keywords— Mobile Ad-Hoc, Symmetric Encryption Algorithm, Integrity, AODV.

I. INTRODUCTION

Ad-hoc networks are characterized by dynamic topology, self-configuration, self-organization, restricted power, temporary network and lack of infrastructure. Characteristics of these networks lead to using them in disaster recovery operation, smart buildings and military battlefields. Routing protocol in ad-hoc networks are classified into three main categories, proactive, reactive and hybride. In proactive routing protocols, routing information of nodes gathered on time when needed. In reactive routing protocol routing information of nodes gathered on time when needed. In hybride the combination of the two are used.

A mobile ad hoc network has following features:

A] Autonomous Terminal:
In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. Besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.

B] Distributed Operation:
For the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.

C] Multihop Routing:
Basic types of ad hoc routing algorithms can be single-hop and multihop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multihop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.

D) Light –weight Terminal:
In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

The cryptographic algorithms are classified into two different types such as symmetric and asymmetric. In symmetric encryption method both sender and receiver share the common key value for encryption and decryption. It requires that the sender find some secure way to deliver the encryption/decryption key to the receiver. The effective key distribution needs to deliver key to the receiver. Large number of protocols provides various techniques. These protocols are to provide more secure but less performance. The public key cryptography or asymmetric cryptographic method solves the problems of key distribution. In this method, uses a pair of keys for encryption. The public key encrypts the data and corresponding private key for decryption. Each user has one pair of keys. The private key kept secret and public key knows by others. Any one wants to send some information to you they read your public key and encrypts the information. After you receive, the encrypted data using your private key to decrypt it. One issue with public key cryptosystems is that users must be constantly vigilant to ensure that they are encrypting to the correct person’s key.
In a public key environment you are assured that the public keys to which you are encrypting data is in fact the public key of the intended receiver. The identification of correct public key of proper person is more difficult without using any third party.

In mobile ad hoc network, each mobile node acts as a host as well as a router. Ad Hoc on Demand Distance Vector routing protocol is a reactive routing protocol which establish a route when a node requires sending data packets. It has the ability of unicast & multicast routing. It uses a destination sequence number (DestSeqNum) which makes it different from other on demand routing protocols. It maintains routing tables, one entry per destination and an entry is discarded if it is not used recently. It establishes route by using RREQ and RREP cycle. If any link failure occurs, it sends report and another RREQ is made. But in existing AODV, there is no reliable security provided for the transmission of the data. MD5, technically called MD5 Message-Digest Algorithm, is a cryptographic hash function. The MD5 cryptographic hash function is most often used to verify that a file has been unaltered by comparing the checksums created after running the algorithm on two seemingly identical packets.

II. SECURITY PROBLEM WITH EXISTING ADHOC ROUTING PROTOCOL

The main assumption of the previously presented ad hoc routing protocols is that all participating nodes do so in good faith and without maliciously disrupting the operation of the protocol [7]. However, the existence of malicious entities cannot be disregarded in any system, especially in open ones like ad hoc networks. In ad hoc network the routing function can be disrupted by internal or external attackers. An internal attacker can be any legitimate participant of the routing protocol. An external attacker is defined as any other entity. Cryptographic solutions can be employed to prevent the impact of external attackers by mutual authentication of the participating nodes through digital signature schemes [9]. However, the underlying protocols should also be considered since an attacker could manipulate a lower level protocol to interrupt a security mechanism in a higher level. Internal attackers having capability to complete access the communication link they are able to advertise false routing information at will and force arbitrary routing decisions on their peers.

III. EXPERIMENTAL PROCEDURE

Module Implementation Status

In phase 1 the tcl script with md5 pure algorithm is compiled by Ns2.35, so that the node scenarios and complete simulation is compiled and this creates a trace file, a nam (network animator) file and a window vs time plotting graph. Using nam-network animator and the nam file generated previously, the simulation can be viewed in the GUI form.

Then the trace file can be used for further processing like generating different graphs with different properties. Then the window vs time graph generated can be viewed using xgraph plugin provided within ns2.

The phase 2 represents the GUI of the simulation where the 100 nodes topology is displayed, here the wireless nodes with range of 550 meters spaced across 800X500 area. Then source and the destination is labeled in the figure above.

The above figure showing the packets dropped when the malicious node try to tamper or copy the packet. Then the remaining nodes across the route receiving that packet is dropped because as the hash value gets changed, so the destination will identify the malicious or tampered packet by mis-combination of hash value generated at the destination and the hash value within the packet and drop it.
In Phase 3, the awk script is used to calculate the statistical information of the simulation using the trace file which was generated by ns2.35. The overall statistic information of the simulation carried is displayed in the above Figure.

I. RESULT SNAPSHOT’S

As, The graph shown above the packets where tampered at the time duration 75 to 78 seconds. As you can see a flat line indicating more latency, so that the packets will be dropped across the route from source to destination.

II. CONCLUSION

The Normal Aodv is altered by using message digest asymmetric key cryptography, to improve the security of such network through the use of MD5-asymmetric Encryption algorithm; This secures the data and also preserves the integrity.

REFERENCES

ACKNOWLEDGMENT

The Whole hearty thank my guide, Sujatha G.N my friends- Srikanth, Kavitha H, Sharath, Harsha and my parents Venkataramanappa and Thayamma and my husband Srinath N for their love, support and encouragement.

AUTHORS

Mrs. Kavitha V
Student,
Department of Computer Science and Engineering,
CMR Institute of Technology,
AECS Layout, Bangalore-563037
Mobile: 9743835278

Mrs. Sujatha S.G
Assistant professor,
Department of Computer Science and Engineering,
CMR Institute of Technology,
AECS Layout, Bangalore-563037
Mobile: 9742128564