iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** VI **Month of publication:** June 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Secure Routing Protocol for Mitigating Adversary Nodes in Mobile Ad-Hoc Networks

Mohammed Adil Adnan [1], Jaganmohana Rao Malla[2]
[1]*B.Tech, (M.E),* [2]*M.Tech ,(Ph.D).*
Department of Electronic and Communication Engineering in Methodist College of Engineering affiliated with Osmania University. Hyderabad

Abstract— The secure routing of MANETs(mobile ad-hoc networks) is still problem in now a day. In this project, a secure routing protocol design for new approach. The existing system says that allowing only legitimate nodes to participate in the bootstrapping process and trying to detect adversary nodes after they are participate in the routing protocol. It does not need secrete channel for route setup. It does not need flooding to setup initial routing. The proposing of existing system, maintain the routes properly in network and detect the adversary nodes whenever enter into network. Here we extend the routes for secure communication from legitimate nodes to controller. We use end to end secure communication protocol and prolonging network lifetime.

Keywords: Ad hoc network, Legitimated nodes, bootstrapping process, Adversary nodes.

I. INTRODUCTION

Mobile Ad hoc Networks (MANETs) is a gathering of wireless nodes which are associated without any infrastructure or any centralized control .In MANET each node can be used as either a send point or as a router to forward packet to next node. In divergence to fixed infrastructure networks, MANETs require fundamental changes to network routing protocols. These are considered by the mobility of nodes, which can move in any direction and at any speed that may lead to arbitrary topology and frequent partition in the network. This characteristic of the MANET makes the routing A challenging issue. In mobile ad hoc network, nodes do not rely of any existing infrastructure. Instead, the Nodes themselves form the network and interconnect through means of wireless communications .Flexibility causes frequent topology changes and may break existing paths. Routing protocols for ad hoc networks can be classified into two major types: proactive and on-demand. Proactive protocols attempt to preserve up-to-date routing information to all nodes by periodically broadcasting topology updates throughout the network. On demand protocols attempt to discover a route only when a route is needed. The general problem of modeling the behavior of the nodes belonging to a mobile network.

.

Figure 1:MANET

II. OVERVIEW OF THE NETWORK

In Networks starts with initial nodes and in first phase the source send the data to user1 and with the help of private key generator (PKG) user2 gets safe packets and then sends back to destination. In second phase when the new node is add in the network setting up the trust value and threshold value of the node in the network.so the higher stated condition make the difference between legitimate node and malicious node in the network. If the malicious node is detected at the same time attack analyzer is built in the network and verify it sends to controller for make flooding technique like MPR(multi point relay).so, legitimate node gets contact

with the other nodes to get route table and mechanism. There will be no difference between the new node and initial node

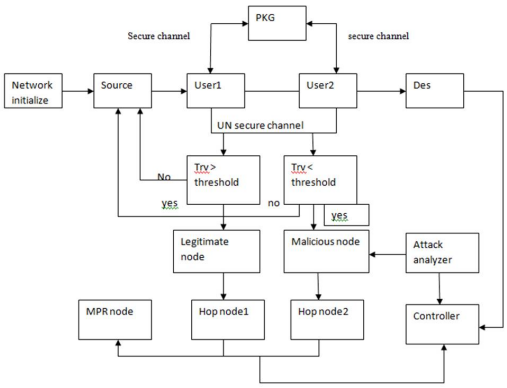


Figure 2: architecture of network

III. AODV ROUTING PROTOCOL USING HASH TECHNIQUE

AODV is a most widely used protocol and it is based on distance vector routing protocol that has been specially build for MANETs. AODV is an on demand protocol and reactive in nature as it finding the routes only when sender wants to send data. AODV makes widespread use of sequence numbers in control packets to avoid the problem of generation of routing loops. When a source node is interested to communicate with a destination node whose route is unknown for sender, it broadcasts a RREQ (Route Request) packet to all its neighbor nodes. Each RREQ packet contains a Request ID, source and the destination node IP addresses and sequence numbers along with a hop count and flags field in its packet format. The Request ID field uniquely identifies the RREQ packet; By observing sequence number field we can have information regarding how fresh the control packet is? And the hop-count maintains the number of intermediate nodes between the source and the destination. Recipient node of the RREQ packet that has not find the Source IP and ID pair or doesn't maintain a fresher (larger sequence number) route to the destination rebroadcasts the same packet after incrementing the hop-count. When the RREQ packet arrived at the destination node a RREP (Route Reply) packet is generated and sent back to the source. RREP packet contains the destination node sequence number, the source and the destination IP addresses, route lifetime along with a hop count and flags. Intermediate node that receives the RREP packet, increments the hop count field, and it establishes a Forward Route to the source of the packet and transmits the packet on the Reverse Route. When a link failure is detected for a next hop of an active route a RERR (Route Error) message is sent to its active neighbors that were using that particular route.

A. Route Request Providing Hash Technique To The Nodes

Route request (RREQ) is initiated by a source node (S) and then propagated by intermediate nodes until the message reaches its destination node (D). On receiving RREQ, an intermediate node I, according to AODV routing protocol, checks whether the message will be re-broadcasted or not. If the message needs to be re-broadcasted and the sender is in node I's neighbor list, it will send (unicast) a message to request the authentication process from the sender: *<AUTHEN RREQ REQ, srcaddr, broadcast id>*. When receiving the authentication request, the sender creates an authentication reply message containing *<AUTHEN RREQ REP, srcaddr, broadcast id, hashKs(RREQ)>*where *hashKs(RREQ)* is the hashed value of RREQ message by the shared key*Ks* between the two nodes. The authentication reply message is unicasted back to node I. Node I on receiving the message will check the integrity of the RREQ message by hashing the message with using the shared key K*s* and then comparing with the received hashed digest. If the comparison is successful (the integrity of the RREQ message is guaranteed), node I continues steps following AODV such as set up reverse path, increase the hop count, rebroadcast the message and so on; otherwise, the RREQ will be discarded. The process continues until the message reaches the destination. The destination also authenticates the sender of RREQ (neighbor of the destination) by the same procedure

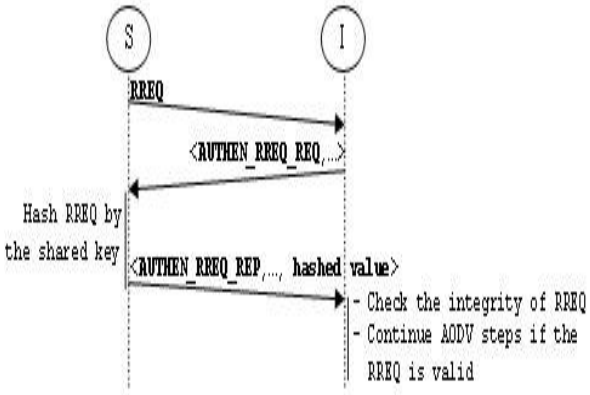


Figure 3: message authentication

B. Route Reply

Route replies (RREP) in AODV are also targets for attacks by malicious nodes. In our schema, when receiving a RREP, a node requests the sender to proof the integrity and non-repudiation of the message by sending an authentication message . The request for authentication is *<AUTHEN RREP REQ, destaddr,destseq #>*and the reply is *<AUTHEN RREP REP, destaddr, destseq #,hashKs(RREP)>*where *hashKs(RREP)* is the hashed value of RREP message by the shared key *Ks* between the two nodes. After the authentication process is successful, a node continues to the steps in AODV, otherwise, the node drops RREP since it is invalid.

In route maintenance process, only route error report message (RERR) is a target for attacks in AODV protocol. Our schema requires the authentication process in sending route error messages to prevent attacks from malicious nodes. The authentication request and response for RERR is *<AUTHEN RERR REQ,unreachable destaddr, unreachable destseq #>*, and *<AUTHEN RERR REP,unreachable destaddr, unreachable destseq #, hashKs(RERR).*

In route maintenance process, because of high mobility it might lose the routing table so to repair the protocol we use OLSR (Optimize Linked State Routing) protocol is used in the AODV routing protocol.

IV. MULTICAST GROUP KEY SUPPORT

Defining a multicast group's private key (receiver key) in align with a multicast group's public key (source key), similar to the one we have used in [9]. In this solution, each multicast group is known by an identification (Multicast Group ID) that is being utilized like an entity ID to obtain the multicast group's public key refer to Identity based cryptography in this approach, each multicast group would have a private key that is managed by PKG and being sent to the Multicast Group Source (MGS) entity. Thus, MGS can grant the membership to a Multicast Group Receiver (MGR) party by providing the multicast group's private key to MGR. Then, MGS encrypts the messages by multicast group's public key and sends them to MGRs while a MGR decrypts the received message with multicast group's private key. Since everybody may find multicast group's public key and be able to send a message, in order to have a source authentication, MGS can signs the messages utilizing its own entity (original) private key (PrK).

V. MULTICAST GROUP SHARED SECRET VALUE

Each multicast group may have its own Pseudo Random Number Generator (PRNG)s͂mi along with the appropriate am & bm shown by equation, and being shared by the multicast group members (source and receivers).

s͂mi+1Ξ (am * s͂mi + bm) mod q

s.t. :i, am , bm , q € Z & s͂mi€ Z*q……(3)

In fact, multicast group members would have two PRNG such as s͂i and s͂mi, which have the similar functional roles. Moreover, they need to use for instance their original secure channel and communication, and set up their group PRNG. As a result, they would have two version of the private key as well. Thus, for the internal multicast group communication and between members, they utilize s͂mi and for the non-multicast communication and to communicate with other non-member parties, they use s͂i.

VI. TRAFFIC CONTROL

Constant Bit Rate (CBR) is a term used in telecommunications, relating to the quality of service. When referring to codec's ,

constant bit rate encoding means that the rate at which a codec's output data should be consumed is constant. CBR is useful for streaming multimedia content on limited capacity channels since it is the maximum bit rate that matters, not the average, so CBR would be used to take advantage of all of the capacity. CBR would not be the optimal choice for storage as it would not allocate enough data for complex sections (resulting in degraded quality) while wasting data on simple sections.

VII.SIMULATION AND RESULTS

All simulation experiments are developed and simulated on intel(R) core i5 with vitual machine using Ubuntu 14.04 with 2 GB RAM and the network simulator NS2 version 2.35

Table:1 is summarized the different configuration values that were used in the performed simulations

Table 1: simulation parameters

PARAMETER	SPECIFICATION
Simulation tools used	NS2 Network Simulator (ns-2.35)
Simulation time	10 sec, 20 sec, 30 sec, and 50sec
Number of nodes	10,20,30,40,50,60,70,80,90,100
Transmission range	250m
Maximum speed	0-20 m/sec
Application traffic	CBR [constant bit rate] [20]
Packet size	512bytes
Node mobility model	10 packets/sec
Protocol	AODV
No. of runs	350

Experiment 1: Network Output

In this experiment we are comparing the two existing and proposed system which is indicating the x-axis we took time and y-axis as number of nodes.

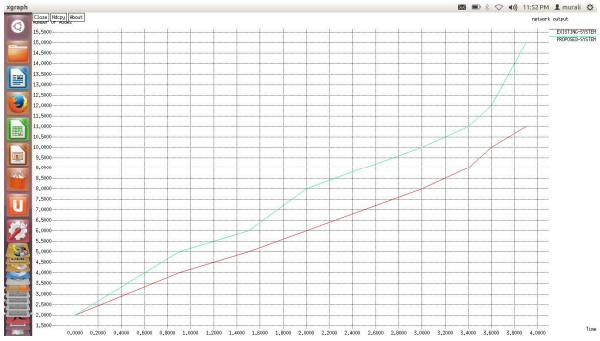


Figure4: Network Output

Experiment 2: packet dropping performance

In this experiment we are comparing the two existing and proposed system which is indicating the x-axis as time and y-axis as number of nodes.

Volume 4 Issue VI, June 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

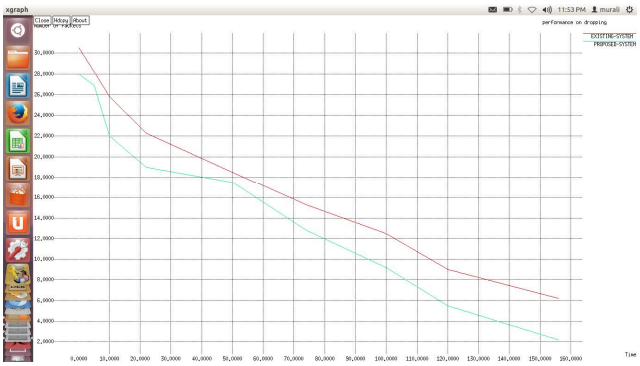


Figure 5: packet dropping performance

Experiment 3: performance of protocols

In this experiments we are comparing the protocols of existing and proposed system which indicating the x-axis as time y-axis as number of nodes.

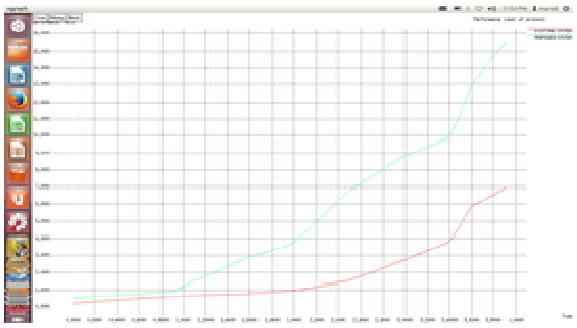


Figure 6: performanace OLSR vs AODV

Experiment 4: performance of delay analysis

In this experiment we are comparing the delay analysis of the existing and proposed system which indicating the x-axis as time and y-axis as number of nodes.

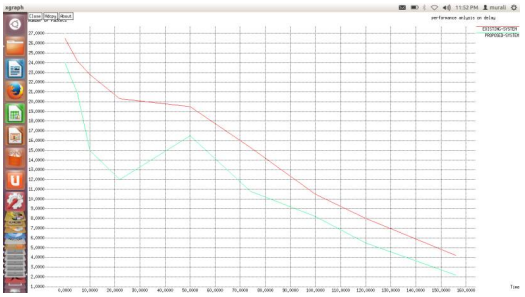


Figure 7: performance of delay analysis

Experiment 5: performance analysis of different densities of mobile nodes.

In this experiment the comparision of different densities we use in this proposed scheme.

Like 15,50,80 nodes are used in this experiment and displayed performance of each density.

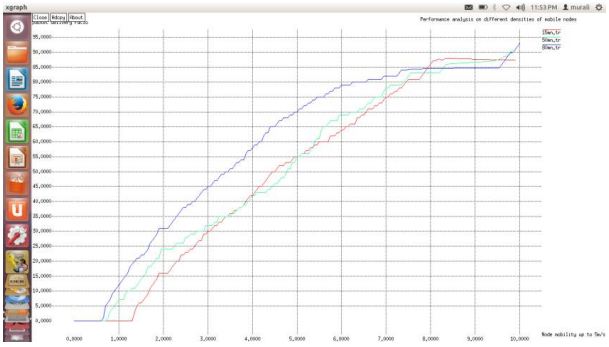


Figure 8: performance analysis of different densities of mobile nodes

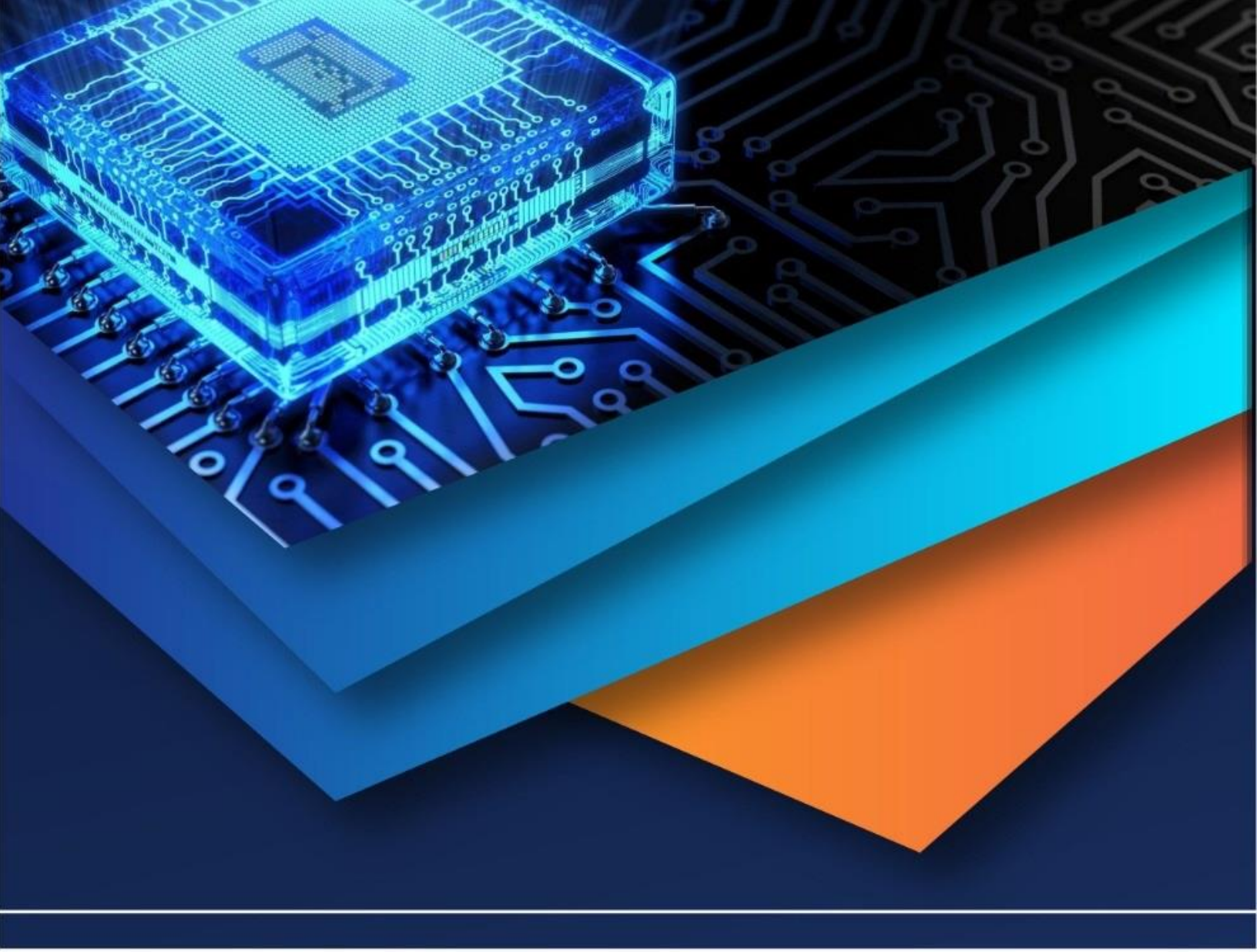
VIII. CONCULSION

The proposed scheme defies various attacks possible in MANETs and satisfies the almost all security requirements in routing protocol with using HASH and multicast key management for this scheme which makes it more easily expandable and less complex in computation. According to simulation that were performed. The newly proposed scheme is based on HASH technique, built on top of normal AODV routing protocol, achieve the good results.

The proposed HASH technique also detect that if any malicious or adversary node in the network. EIBC maintain the routes properly in network and detect the adversary nodes whenever enter into network. Here we extend the routes for secure communication from legitimate nodes to controller.

REFERENCES

[1] Shamir, ”Identity-based Cryptosystems and Signature Schemes,” Advances in Cryptology - CRYPTO, LNCS 196, pages 47-53, Springer- Verlag, 1984.
[2] H. Nicanfar, P. Jokar and V. C.M. Leung, ”Efficient Authentication and Key Management for the Home Area Network,” to be presented at IEEE ICC Conference, Ottawa, ON, June 2012.
[3] Enhanced Identity-Based Cryptography, a Conceptual Design Hasen Nicanfar and Victor C.M. Leung, Systems Conference (SysCon), 2012 IEEE International.
[4] Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-hoc Networks Arshad, J.; Azad, M.A. Sensor and Ad Hoc Communications and Networks, 2006. SECON '06. 2006 3rd Annual IEEE Communications Society on Year: 2006
[5] Securing AODV Routing Protocol in Mobile Ad-Hoc Networks ”Phung Huu Phu, Myeongjae Yi, and Myung-Kyun Kim”
[6] Introduction to Network Simulator NS2, Teerawat Issariyakul, Ekram Hossain, Springer, 1st edition, 2008
[7] Goldwasser, S. and Bellare, M. "Lecture Notes on Cryptography". Summer course on cryptography, MIT.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY