APPROACH FOR RECIPROCITY OF KEY FOR SECURE ROUTING IN MANETS

Amita Ram Kulkarni[1], Raghavendar Raju L[2], Surya Kumar L.[3]
[1&3]UG Student, [2]Assistant professor
[1,2,3]Department of Computer Science and Engineering, Matrusri Engineering College, Saidabad, Hyderabad, India.

Abstract-- MANET is a set of ad-hoc wireless devices with limited broadcast orbit and resources. Communication is accomplished by relaying data along suitable routes that are dynamically determined and preserved through collaboration between the nodes. Find of such routes is a principal task, both from efficiency and security point of aspects. This paper presents an efficient and secure routing, based on asymmetric authentication using Approach of Reciprocity Key (AKR). The proposed mechanism ensures secure routing by also taking the Quality of Service (QoS) in MANETs and minimizes the network overhead. The AKR performance can be efficaciously used to create a new routing protocol for Mobile Adhoc Networks which will provide maximum security against all kinds of attacks. In this paper, AKR is compared with other secure routing protocols like TWOACK, and AODV, to evaluate the efficiency of AKR in Ad Hoc Networks. The empirical results show that there is an increase of 22% packet delivery ratio and a decrease of 9% routing overhead.

Index Terms-- **MANETs, AKR, Security, Routing, key.**

I. INTRODUCTION

MANETs [3] are Mobile ad hoc [6] networks and the name by itself gives us the brief meaning of the concept. These networks are essentially the ones which are temporary and mobile, i.e. they can be formed at any instance and the nodes in the network are movable. Hence, the topology of the network changes from time to time.
Routing is the process of finding route between the source node and destination node in the network. Routing issues include unauthorized destination nodes, loss in the data packets, unauthenticated nodes in the network are some of the routing issues which cause disturbance in the network. By using the routing protocol such as reactive routing protocol the network overload is reduced and packet delivery ratio increases.

The ARK technique eradicates all the routing issues in the network which were mentioned in the above section. Most of the networks are attacked by external and internal attacks which are difficult to be discovered. It uses Authority for Certification in order to authenticate and certify the nodes. This research paper aims at resolving the issues like loss of packets and disorder in sequence of the packets at the destination. ARK plausibly minimizes the routing relay and increases the packet delivery ratio at a maximum extent.

II. RELATED WORKS

K. Liu et al. [8] has proposed TWOACK which is one of the most important approaches for detection of intruders in MANETs. TWOACK provides detection of misbehaving of links by acknowl44 http://www.i-jim.org Paper—A Key Exchange Approach for Proficient and Secure Routing in Mobile Adhoc Networks involves every data packet to be transmitted over every three approaching consecutive nodes along the path from the source node to the destination node. Upon the retrieving the packet, each node along the route should send back an acknowledgment packet to the node that is two hops away from the route. TWOACK should work on routing protocols like Dynamic Source Routing (DSR).

Liu et al. [9] shows how the networked nodes autonomously support as well as cooperate with each other in a peer-to-peer (P2P) configuration to quickly discover and self-configure any services which are available on the area of disturbance and deliver a real-time capability by self-organization among themselves in dynamic groups for providing higher flexibility and adaptability for monitoring the disturbance and providing relief.

Latvakoski et al. [7] explains a concept of communication architecture for dynamic systems, integration of application-level dynamic group communication, and ad hoc networking together. A set of methods are required to enable plug and play, addressing and mobility, peer to peer connectivity and the usage of different services are also to be provided.

This research paper implies the amalgamation of the all the works mentioned above and enhances the process of reciprocity of key in a stable network by improving the security and QoS parameters. It helps in removing or reducing the routing overlay and increasing the packet delivery ratio.

III. APPROACH FOR RECIPROCITY OF KEY(ARK)

To achieve a reliable communication and to have node authorization in mobile ad hoc networks(MANETs), Approach of Reciprocity key exchange (ARK) for node authorization and user authentication is needed. We have proposed a secure and proficient routing approach using key exchange approach. In ad hoc routing, nodes exchange information to their neighbor nodes and construct a virtual network for data packet routing to be delivered to their desired destination. This information is very likely to get targeted by malicious adversaries who intend to disturb the functionality of the network. Attackers insert erroneous routing information externally like repeating the previous messages or make modifications to the original and weaken the network. Internal attacks can cause severe damage to the networks. Nodes may also send erroneous information to disrupt the network topology. It is also practically difficult to identify the attacker and hence it is reasonable to make the routing secure in advance so that there are no chances of the attacker causing disturbance in the network.

- **Acquisition of Key**

In this we use the symmetric keys, i.e. only one key is used for both Encryption and Decryption. Among all the nodes in the network we assign keys to few or many of the nodes. An entity called Authority for Certification(AC) is used to authorize every node in the network so that there will be no entry for the malicious nodes or any other adversaries. With the help of AC, we can also identify the malicious nodes before giving them the certificate for authentication and authorization. AC generally distributes ‘certificates’ to the neighbouring nodes. The neighbouring nodes in return provide their identity to the AC after the AC issues the certificates to them. Any node which provides false information regarding its identity will be thrown away from the network or will be isolated. The certificate issued for node ‘ND’ can be stated as follows:

C_N= $Encrypt_{AC}$ (ND_{add}, ND_{pub_key}, ND_{pvt_key}, AC_{pub_key})

B. Process of Secured Routing

Discovering the Neighbours: The proposed Approach for Reciprocity of Key(ARK) performs a neighbor discovery by broadcasting a ‘Hello’ message within a limited or bounded communication range. This message is sent to the nodes which are at a distance of 1-hop from the source node. Through this idea of 1-hop nodes we can significantly reduce the power consumption. Then the source node receives a reply from the nodes which have received the messages as an acknowledgement. In return the source node receives the nodes’ public key and a message signature for identification of the node for authorization.

Method 1: NeighNodes(V)

```
Assign msg= “Hi”
Broadcast msg in network to discover NeighNodes which are secure
While min discovered
A signed message is received from the NeighNodes -> $N_{sign}$
      If path==1-hops then
            GenSign(msg)-> $V_{sign}$
            If validateSign($V_{sign}$, $N_{sign}$)==true then
                  Add node addr to RouteTable->R_Nodes(N)
                  Add node pub_key to NodeTable->N_Key[N, $N_{pubkey}$]
            End if
      End if
End While
```

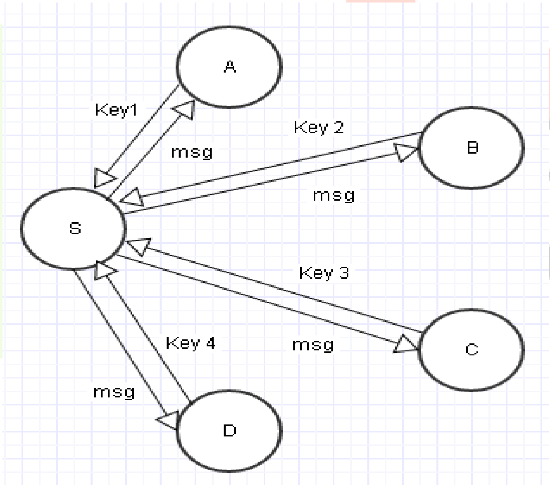

Fig.1. Discovering the neighbour for secure routing

Discovering Routes Securely: It is important to always have a secure route apart from having a short route. For this process, we maintain a routing table Route which are identified by the Neighbour Discovery process must be secured enough to start the process of sending message from the source to the destination. The 1-hop nodes must be identified, authorized and secured to prevent any intruders from even thinking of entering the network. If nodes generate an invalid signature then the node must be isolated from the network. After the completion of secure route discovery, the optimal route is stored in the routing table. The data packets ae sent from the source to the destination nodes considering the number of hops. The usage of 1-hop nodes reduces the overhead which is a prominent problem in the multi-hop nodes. These following phases are involved for discovery of secured routes:

1) **Route discovery phase:** A RREQ (Route request) packet is broadcast via the method of flooding to all the neighbours. The broadcast ID gets incremented each time a source uses RREQ packet. Broadcast ID and Source IP address together form a unique identifier for the RREQ packet. Each node receiving RREQ forwards RREQ to its neighbors if it is not the destination node. If it is the destination node or the node which knows recent path to destination, it sends back RREP to the sender. Sequence number is used to make sure that duplicate packets do not arrive at the destination.

2) **Data Transmission phase:** After getting the route information from source to destination it begins to forward the data to the route with the least number of hop counts possible.

3) **Route maintenance phase:** If data transmission fails due to breakage of link then the Route maintenance method comes into picture. The last node of link breakage will process the method of Route discovery.

IV. EXPERMENTAL EVALUATION

A. Simulation Methodology

General case methodology: Here, we have simulated a packet dropping attack where the malicious nodes just directly reject the packets and drop them all packets they receive. In this case the objective is to test the performance of the protocols we are using against the secure protocols which exist.

B. Simulation Setup

The comparison of ARK with AODV and TWO-ACK is done for evaluation. The network scenario is run twice and average performance is calculated.

Table1. Simulation Parameters

Configuration	Parameter Values
Simulation Area	1000m X 1000m
No. of Nodes	50
Mobility Speed	0 to 20 m/s
Source-Destination Pairs	15
Packet Size	512 bytes
CBR Rates	4 pkts/sec
Mobility	RWP
Pause Time (sec)	100
Malicious (%)	0, 10, 20, 30, 40, 50

C. Performance Evaluation

We provide a comparison of the analysis of the performance for a better vision of the results of our simulation that are provided in the case we have specified. In our case, the malicious nodes reject all the packets which pass through them.

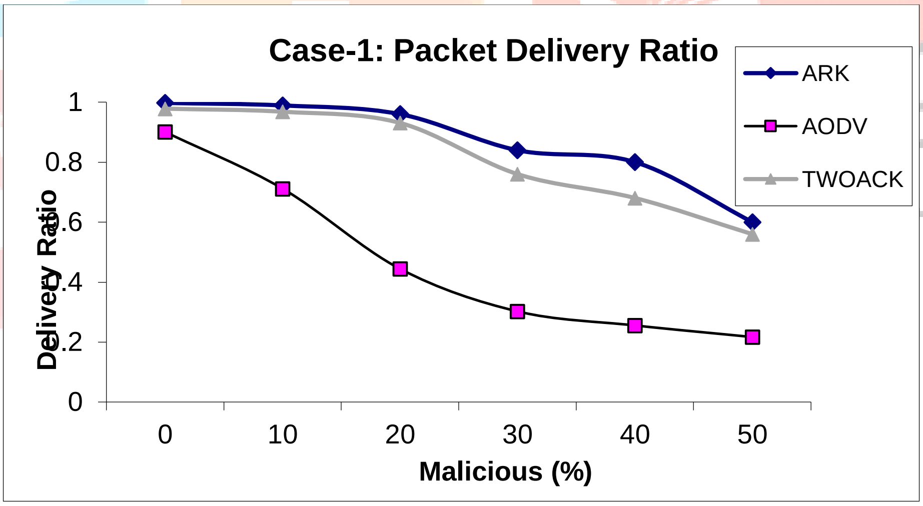

Fig.2. Packet Delivery Ratio Comparison

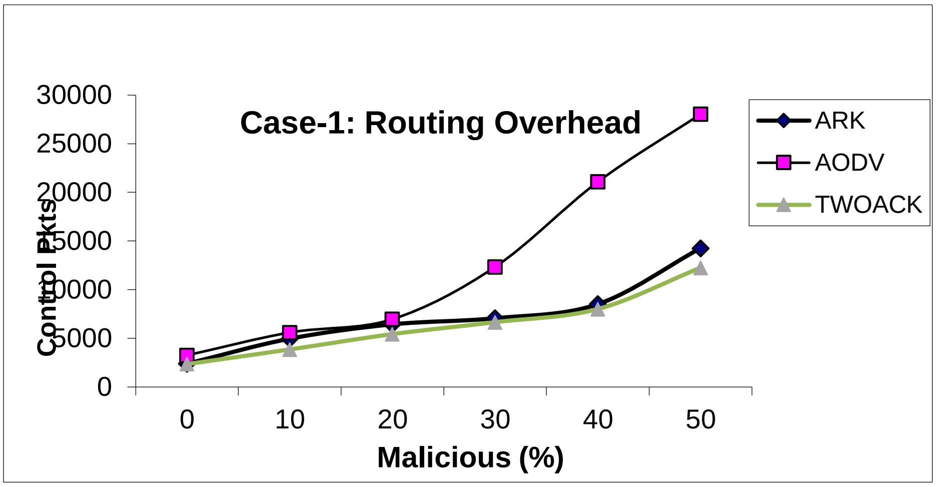

Fig.3.Packet Delivery Ratio Comparison

Here, in figures 1 and 2 ARK shows high PDR and AODV is seen to be low. ARK shows an improvement of 22% in PDR. This improvement is achieved due to the Secure Neighbour Node Identification Mechanism, which helps ARK to obtain a secure route for delivering high number of packets.

V. CONCLUSION

This paper about the Approach for Reciprocity of Key(ARK) is proposed for proficient and secure routing protocol for MANETs. This authenticates the messages that are being routed using the digitalized signatures that are based on asymmetric cryptography. The capability of ARK is the determine a safe and secure path. The establishment of security of the route found is done through a message signature received during the discovery of the neighbor nodes. The secure node identification mechanism for authenticity and route discovery helps for the improving of the throughput of the packet delivery ratio during the working of the communication. The result we obtain shows a 22% increase in PDR with a very small amount of overhead about 9%. By this we minimize all the packet delay and routing relay mechanisms and there is optimization for reducing further overhead caused by routing in comparison with others.

REFERENCES

[1] A Survey on Routing Protocols and QoS in Mobile Ad Hoc Networks (MANETs), L. Raghavendar Raju and C. R. K. Reddy
[2] A key management and secure routing integrated framework for Mobile Ad-hoc Networks, Shushan Zhao, Robert Kent, Akshai Aggarwal
[3] A Key Exchange Approach for Proficient and Secure Routing in Mobile Ad hoc Networks, L. Raghavendar Raju and C. R. K. Reddy
[4] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions On Industrial Electronics, Vol. 60,No.3, March 2013 https://doi.org/10.1109/TIE.2012.2196010
[5] Feeney L.M., B. Ahlgren, A. Westerlund, and A. Dunkels, "Spontnet: Experiences in Configuring and Securing Small Ad Hoc Networks", Proc. Fifth Int'l Workshop Network Appliances, Oct. 2002.
[6] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Proc. 8th Ann. Int'l Conf. Mobile Computing and Networking (MobiCom 2002), ACM Press, 2002, pp. 12–23. https://doi.org/10.1145/570645.570648
[7] Latvakoski J., D. Pakkala, and P. Paakkonen, "A Communication Architecture for Spontaneous Systems", IEEE Wireless Comm., vol. 11, no. 3, pp. 36-42, June 2004.https://doi.org/10.1109/MWC.2004.1308947
[8] L. Liu, J. Xu, N. Antonopoulos, J. Li, and K. Wu, "Adaptive Service Discovery on Service-Oriented and Spontaneous Sensor Systems", Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/2, pp. 107-132, 2012.
[9] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs", IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007. https://doi.org/10.1109/TMC.2007.1036