Enhanced QoS Based on Secure Reliable Key Routing Mechanism in Mobile Adhoc Network

V.L. Pavani, B. Sathyanarayana

Abstract—Ad hoc wireless network is experiencing challenges due to various security issues and resource constraints in nature high mobility. There is always the challenge to create a reliable and optimized network for efficient routing. Ensuring a dynamic way that path which is known in communications is always a challenge in the mobile ad hoc network. Most of the existing secure routing protocols will target a particular type of malicious attacks or behavior of network. We propose a secure reliable key routing (SRKR) mechanism for secure and dynamic routing in mobile adhoc network for enhancing the QoS. It defines a unique reliable key for each communication route to perform a securing data packets routing using asymmetric cryptography and secure encrypted message routing. We evaluate the proposal through simulated experiments in different mobility scenario in a network. Simulation results shows an enhancement in QoS through achieving high throughput over existing approaches.

Index Terms—Security, Quality of service, Reliable key, Routing, Cryptography, MANET.

1 Introduction

MOBILE ad-hoc network, offers a unique advantage and versatility for the wireless environment and its applications. This does not require any fixed infrastructure, including the prerequisite of a base station. But at the same time it is, in its dynamic nature and inadequate protection system, is vulnerable than traditional wired network [1][22]. As the boundary of operation is not limited to the topology, it has strong possibility essentially impaired. This is because, in order to maintain any centralized policy or scheme of the conventional network, it is very difficult to ensure an ad hoc routing of that difficulty. Many of ad hoc routing protocols, have been proposed in the past [11][13], very few of the proposals has been dealing with the security requirements to target the high vulnerability in the ad hoc network[2]. Resources in MANET in addition to the above difficulties, creates the problem of the deployment of the security process, it is a major constraint. AODV [12] and in the DSR [8] routing is very efficient, but both has been the prone to various types of attacks.

In this paper, we present secure reliable key routing (SRKR) mechanism modifying conventional AODV to tackle the security challenges in MANET. In SRKR, all routes to the destination securely trusted with a unique reliable key which is a novel contribution in this work. It provides a secure communication approach in which messages are secured using symmetric encryption and routing with authentication.It secures the data using a unique reliable encryption key which is created using a trusted path. This has the advantage of enhancing the QoS at such with a high throughput and less end-to-end delay in a low cost routing constraints.

To evalauate the proposal we compared SRKR with AODV, Authenticated Routing for Ad hoc Networks (ARAN)[6] and Secure-AODV(S-AODV) [5].

The rest of the paper organized in sections, Section-2, describes the related work which provides an overview on AODV, ARAN and S-AODV routing protocols. In Section-3, we describe the secure reliable key routing mechanism, Section-4 describes the experiment and results evaluation and Conclusions in Section-5.

2 Related Works

The number of ad hoc routing protocols are presented in [7] [9] [10] [20] [21] with a security vulnerability are due to communication environment and wide open, and these vulnerabilities [23] are common in mobile ad hoc routing protocols. In this paper, to overcome these vulnerabilities problem we discussed AODV, ARAN and S-AODV.

2.1 AODV - (Adhoc On-demand Distance Vector routing protocol)

AODV [12] is a reactive routing protocol for mobile ad hoc network, which build route on demand. It offers lower network overhead and uses the sequence numbers to ensure the prevention of routing loop. Basically, it uses three kinds of messages to carry out communication and maintenance as RREQ, RREP and RRER. It uses table driven routing mechanism for routing data packets to the destination nodes.

Securing the routing messages is a major concern in the AODV routing. It requires authentication to ensure the sender and recipient of the message. Each node in the request broadcast check the number of initiator sequence in the message RREQ against stored information in the routing table, if it finds a new request it update the routing table. For a route reply it checks the destination node sequence number instead of checking the number of the originator and keep Routing Information updated. Its vulnerability attacks results in

- *V.L. Pavani, Research Scholar, Department of Computer Science and Technology, Sri Krishnadevaraya University, Anantapur, Andhra Pradesh, India. E-mail: pavaniveluru1@gmail.com*
- *B. Sathyanarayana,Professor, Department of Computer Science and Technology, Sri Krishnadevaraya University, Anantapur, Andhra Pradesh, India.*

routing loops, message modification, spoofing and many other attacks which are serious to AODV protocol.

2.2 ARAN - (Authenticated Routing for Adhoc Networks)

Sazgiri, et.al. propose ARAN[6] for securing routing mechanism from unauthorized participation, route modification, spoofing, message modification etc. ARAN is based on an on-demand routing protocol extends the features of AODV protocol. It provides route message integrity and non-repudiation as minimal part of the security policy for MANET.

ARAN proposes security process in three stages as, preliminary certificate process, end-to-end authentication and secure optimal shortest path. It used trusted certificate server TC and public key cryptography to implement the three stages. Each node must acquire certificate form TC before joining the network.

The authentication scheme of the ARAN provides protections against route or message modification, fabrication and impersonation. A launch of denial-of-service attack by a group of malicious node by simply broadcasting large number of route denial packets exhaust the computational resource to verify the signature and then generate a new ones. This drawback of ARAN utilizes extra bandwidth to transmitting certificate creates more routing overhead. ARAN also fails to detect internal attacks as all nodes in network trust each other for cooperation in providing stable communication[14][15] and it might create huge disturbance in case of malicious node presence.

2.3 S-AODV - (Secure-AODV)

Zapata, et. al[5] propose Secure -AODV to secure the AODV routing protocol due to numerous security vulnerabilities in the protocol as it can allow a malicious intermediate node for spoofing its identity illegally and modify the hop count on route request messages and also can fabricates route error messages.

SAODV is an extension of AODV protocol which is based on public key cryptography to provide routing security. It uses RREQ, RREP and RERR as routing messages which are digitally signed, in order to secure the guarantee the integrity and authenticity. Every time a node that generates a routing message signs it with its private key, and the nodes that receive this message verify the signature using the sender's public key to authenticate. The hop count cannot be signed by the sender, because it must be incremented at every hop. Therefore, in order to protect it a mechanism based on hash chains is used.

It generates bigger messages due to heavy weight symmetric cryptography used for digital signature. Every time the messages received by the intermediate nodes must verify signature for authentication. It increase an over burden when the double signature mechanism is used for a single message for generation and verification.

3 Secure Reliable Key Routing Mechanism

In ad hoc routing protocol nodes exchange information to their neighbourhood and build a virtual network for routing data packets to their desired destination. Such informations are easily can be targeted by any malicious adversary who intentionally want to disrupt network functionality. Attackers usually inject externally erroneous routing information to repeat previous routing messages, or edit valid routing information and eventually bring the network down. Sometimes internal attacks cause severe damage as these nodes are not up to their initial commitments. These nodes can also send wrong information to modify the local view of the network. Usually, it is very difficult to identify the internal attacker, since we already have some kind of credentials that everyone believes.

SRKR target both external and internal attacks that can occur in the network because of malicious nodes. It identifies these attacks, based on the three security mechanism, Certificate Acquisition, Secure Discovery of Route and Secure Data Routing. It uses the Certificate Authority (CA) certificates to identify internal attackers and use both symmetric and asymmetric encryption to secure from external attackers. To prevent routing information from forged or tampered with, we use CA certificates for encrypting messages.

3.1 Acquisition of Certificate

Establishing a security association between the mobile nodes is the most difficult part of an ad hoc network. The difficulty is due to the nature of mobile ad hoc networks, where a pre-defined architecture for safety cannot be used. Most work-related security association and key distribution were not addressed well in most of the previous secure routing protocols. One of the simplest solutions is described in [16], for the existence of a security association between the source and target nodes. Exchange of group key is described in [17], which is based on a strong key sharing, but this approach requires nodes of the static and dynamic networks where a node join and leave very often the key groups should be updated in the process for all nodes.

In [18][19] describes another security association process among the nodes which use asymmetric cryptography where any node in the network can issue certificate for a new nodes. This is a strong approach in sense of that it does not have any single point failure in the network. But it still can have vulnerability attacks as to authenticate a new node and issue a certificate is risky if malicious nodes are already present in the network.

In SRKR protocol, to have an initial security association among the node we also distribute the certificates. But these certificates are obtained from a trusted certified authority (CA), and it has to be loaded to each node prior to join the network. This will be an offline process where each node by providing their identity to CA needs to obtain their certificate. In this approach if any node tries to possess an invalid certificate illegally can be identified and isolated easily. The certificate issued by the *CA* for a node *V* will be consists of CA public key as CA_{pub_key}, node address as V_{add} , public key as V_{pub_key} and private key as V_{pvt_key} . The certificate represented as,

$$C_V = E_{CA_{pkey}}[V_{add}, V_{pub_{key}}, V_{pvt_{key}}, CA_{pub_{key}}]$$

We assume that all the valid nodes in the network obtain this certificate before joining the network. This process of acquiring certificate provides the basic identification to the node and prevent from internal malicious.

3.2 Secure Route Discovery Mechanism

Our protocol modifies AODV routing protocol to provide the secure routing mechanism. AODV is a reactive protocol, it accomplish its communication through route discovery, data routing and route maintenance process.

Whenever a source node *N* wants to communicate with a destination node *D* in the network, it initiates route discovery process in form of sending RREQ message. To make discovery process secure SRKR creates a reliable key using Diffie-Hellman algorithm as R_{key}, create encrypted message signature using SHA1 algorithm as E_{msg_sign} and encrypted message cipher using CA_{pub_key} as E_{msg}. Before broadcasting the message again encrypted using CA_{pub_key} as shown in equation-1. The idea of encrypting message twice makes it highly secure from both internal and external attackers. The broadcast message with timestamp *T* represent as,

$$M_{Req} = E_{CA_{pub\_key}}[E_{msg\_sign}, E_{msg}, R_{key}, D_{add}, T] \qquad -(1)$$

Therefore, the SRKR protocol is capable of determining secure route by comparing the security parameters while performing route discovery of each individual node. The mechanism of the route discovery is described in Algorithm 1.

Algorithm 1: SRKR Secure Route Discovery Mechanism

Source Node *V* init RREQ -> Init_Request(V_{rreq})

Method1: *Init_Request(Node$_{rreq}$)*

```
V Create Reliable key using DH Algorithm → $R_{SKey}$
V Encrypt(Msg) using SAH1 Algorithm → $E_{msg\_sign}$
V Encrypt(Msg) using $CA_{pub\_key}$ → $E_{msg}$.
V Encrypt([$E_{msg\_sign}$ , $E_{msg}$ , $R_{SKey}$ , $D_{add}$, T ]) using $CA_{pub\_key}$ → $M_{rreq}$
V broadcast $M_{rreq}$ to all neighbouring node(N)
while $N_i$ is not destination node → $D_{add}$ do
    $N_i$ Decrypt($M_{rreq}$) using $CA_{pvt\_key}$ → [$E_{msg\_sign}$ , $E_{msg}$ , $R_{SKey}$ , $D_{add}$, T]
    $N_i$ Decrypt($E_{msg}$) using $CA_{pvt\_key}$ → Msg
    $N_i$ Encrypt(Msg) using SAH1 Algorithm → $IE_{msg\_sign}$
    If validateSignature ($IE_{msg\_sign}$ , $E_{msg\_sign}$ ) == true then
        If Msg == 'RREQ' then
            If $N_i$ == $D_{add}$ then
                D Store Source Reliable key($R_{SKey}$) → Destination_Table
                Destination Node D → Init_Reply($D_{add}$).
            Else
                $N_i$ Append $I_{add}$ fields data → Append($M_{rreq}$, $I_{add}$) → M
                $N_i$ Encrypt(M) using $CA_{pub\_key}$ → $M_{rreq}$
                $N_i$ broadcast $M_{rreq}$ to all its neighbouring nodes (N)
            End if
        End if
    End if
End while
```

Method2: *Init_Reply(Destadd)*

```
D Creates Destination Reliable key using $R_{SKey}$ and DH Algorithm → $D_{SKey}$
D Encrypt(Msg) using SAH1 Algorithm → $D_{msg\_sign}$
D Encrypt(Msg) using $CA_{pub\_key}$ → $E_{msg}$.
D Encrypt([$D_{msg\_sign}$ , $E_{msg}$ , $D_{SKey}$ , $S_{add}$, $S_{Path}$ , T]) using $CA_{pub\_key}$ → $M_{rrep}$
D unicast $M_{rrep}$ to the route node (N) from which it receive RREQ.
While $N_i$ is not source node → $S_{add}$ do
    $N_i$ Decrypt($M_{rrep}$) using $CA_{pvt\_key}$ -> M as [$D_{msg\_sign}$ , $E_{msg}$ , $D_{SKey}$ , $S_{add}$, $S_{Path}$ , T]
    $N_i$ Decrypt($E_{msg}$) using $CA_{pvt\_key}$ → Msg
    $N_i$ Encrypt(Msg) using SAH1 Algorithm → $IE_{msg\_sign}$
    If validateSignature ($IE_{msg\_sign}$ , $D_{msg\_sign}$ ) == true then
        If Msg == 'RREP' then
            If $N_i$ == $S_{add}$ then
                Source Node V store destination Reliable key($D_{SKey}$) → Routing_Table
            Else
                $N_i$ Read Source Path from M → $S_{Path}$
                $N_i$ Read next hop from the $S_{Path}$ → $Next_{Hop}$
                $N_i$ unicast $M_{rrep}$ → $Next_{Hop}$ ($N_i$)
            End if
        End if
    End if
End while
```

3.2 Data Routing Based on SRKR Mechanism

On successful completion of secure route discovery, Source node sends data packet on the optimal route stored in the routing table. Generally AODV protocol maintains only one route from source to destination. In our scheme we also maintain the same, as multi-route discovery expense more overhead of storing more route information. Before sending the data packet source make data packet secure. To do so, source node generate a unique secret key as SC_{Key} using destination Reliable key, D_{SKey} of DH algorithm which is received during route discovery process. It encrypt the data packets using SC_{Key} and route the packets.

Using this mechanism SRKR protocol is capable of securing its data packets during data routing in a route. The mechanism achieved using method-1 and 2 of the secure data routing as described in Algorithm 2.

Algorithm 2: SRKR Secure Data Routing Mechanism

Source node *V* init data transmission -> *SendData*(D_{add}, *pkt_seq_no*)

Method1: ***SendData(Destination$_{add}$)***

```
$V$ gets the discovered route → $R_{Path}$
$V$ gets destination Reliable key → $D_{SKey}$
$V$ generate unique Secret key using $D_{SKey}$ → $SC_{Key}$
For "number of data packet to send" loop
    $V$ creates Data Packet → $D_{pack}$
    $V$ Encrypt data packet using secret key -> Encrypt ($D_{pack}$ , $SC_{Key}$ ) → $E_M$
    $V$ sends encrypted data packet $E_M$ → $Next_{Hop}$
    while "ACK_Time expires" do
        If "Receive Message → $E_M$" then
            $V$ gets its own Reliable key → $S_{SKey}$
            $S$ generate unique Secret key using $S_{SKey}$ → $SC_{Key}$
            $S$ decrypt the data packets using $SC_{Key}$ → Decrypt($E_M$ , $S_{SKey}$ ) → $D_M$
            If $D_M$ =="DELV_ACK" then
                End while;
                Send next data packet → SendData($D_{add}$, pkt_seq_no)
        Else if "ACK_Time expires" then
            Resend the data packet → SendData($D_{add}$, pkt_seq_no)
        End if
    End while
End for
```

Method2: ***RecieveData(E_M, pkt_seq_no)***

```
Destination node $D$ on receiving the data packets,
$D$ gets its own Reliable key → $D_{SKey}$
$D$ generate unique Secret key using $D_{SKey}$ → $SC_{Key}$
$D$ decrypt the data packets using $SC_{Key}$ → Decrypt($E_M$ , $D_{SKey}$ ) -> $D_M$
$D$ gets its Source Reliable key → $S_{SKey}$
$D$ generate unique Secret key using $S_{SKey}$ → $SC_{Key}$
$D$ decrypt the DELV_ACK message using $SC_{Key}$ → Decrypt(DEL_ACK , $D_{SKey}$ ) → $E_M$
$D$ Sends secure acknowledge $E_M$ back to source.
```

We investigate the possible attacks [23] in the route discovery and routing and countermeasures that are taken in SRKR to secure routing in mobile adhoc network.

A. Attacks on Route Discovery Process

- *Route Message Modification:* Route process discovery require intermediate node cooperation to discover the route to destination. An attack on the intermediate node may leads to route message modification. To handle this kind SRKR encrypts the route message symmetrically using SHA1 algorithm and asymmetrically using node public key. It provides a double shielding for attackers to through pass to perform route message modification, which is a novel contribution of this work.

- *Route Cache Poisoning:* This kind of attack misguides the node to route data in incorrect path. SRKR handles this attack using Reliable key created by both source and destination. A malicious node broadcast incorrect paths has no effects on route cache, firstly each route request message is highly secured and protected by Reliable key and node public key and secondly the unique reliable key make the message completely indifferent from the regular route message.

- *Not Participating in Discovery Process:* Not participating in route discovery or dropping a packet is a passive malicious attribute which will not interrupt the discovery process until there are non-malicious nodes are available in the network. To handle this kind of behaviour SRKR insure each node participating must have identity and CA certificate.

B. Attacks on Data Routing Process

- *Data Packet Modification:* During data communication it is always possible that intermediate node can inject false route by modifying the data packet information to degrade the throughput. SRKR handles data packet modification by encrypting data packets using unique secret key during routing. Both source and destination node create unique secret key for sending data packets and informing acknowledgement message.

- *Data Packet Dropping:* Data packet dropping is a common behaviour of malicious nodes which impacts the performance of network. To handle this kind of attack SRKR protocol ensue that trusted and CA certified node must participate in communication process.

4 Experiment Results

To evaluate our proposal we assume that both internal and external types of malicious nodes are exists. However, we also assume that the most of the nodes present in the network are trustable due to certification acquisition form CA. We use node public key cryptography to protect the network against the external attacks and symmetric cryptography encryption for data and message protection from internal attacks. We experimentally simulate SRKR protocol using Glomosim Simulator[x] to evaluate the performance. It provides scalable and parameter driven environment for wireless protocol simulation. We compare the performance of SRKR with S-AODV [4] and ARAN [6] for evaluation.

4.1 Network Setup

To simulate the protocol we setup the parameter described in the Table-1. The simulation runs on Random Way-point model with a speeds variation up to 100 m/s. We perform the simulation in two sets. First set does not have any malicious node while second set contains 40% of malicious nodes.

Table-1: Simulation Parameters

Configuration	Parameter Values
Simulation Area	1000m X 1000m
No. of Nodes	50
Pause Time	30 sec
Source-Destination Pairs	25
Packet Size	512 bytes
CBR Rates	4 pkts/sec
Mobility	RWP
Mobility Speed (m/s)	0,20,40,60,80,100

During route discovery process all nodes behave normally as they are certified. During data routing we configure the simulator to choose 40% node as malicious randomly. It was observed that those nodes behave abnormally and tries to modify data packets and tries drops all data packets routed through them.

4.2 Experiment Results

Throughput: Figure-1(A) and (B) shows the throughput performances of the protocol. All protocols show similar result in case of absence of malicious node. SRKR shows an improvisation in compare to others protocols schemes in presence of malicious nodes. The improvisation of throughput is due to the efficient securing of the data packets from attacks. In absence of malicious it shows an average performance due to cryptography overhead. SRKR achieves 25 % improvisation of packet delivery in compare to other protocols where as others shows a downfall of 10-20% in case of 40% malicious presence.

End-to-End delay: Figure-2(A) and (B) shows end-to-end delay comparison between SRKR and others protocols. All the protocols shows similar ratio of increase in delay with increase of mobility speed in absence of malicious node. But in case of malicious presence SRKR and ARAN shows low delay in compare to other protocols. Both ARAN and SRKR follow the process of certificate acquisition which allow secure and identified node in network, which helps in minimizing packet drop and end-to-end delay in case of malicious attacks.

Control Overhead: Figure-3(A) and (B) shows control overhead comparison between SRKR with others protocols. In absence of malicious node all the protocol have similar ration overhead. But in case of malicious presence SRKR shows low routing overhead in compare to others, because SRKR encrypt and decrypt data packets only at source and destination end during data communication, where as in other protocol security checks are perform during communication which increase the routing overhead.

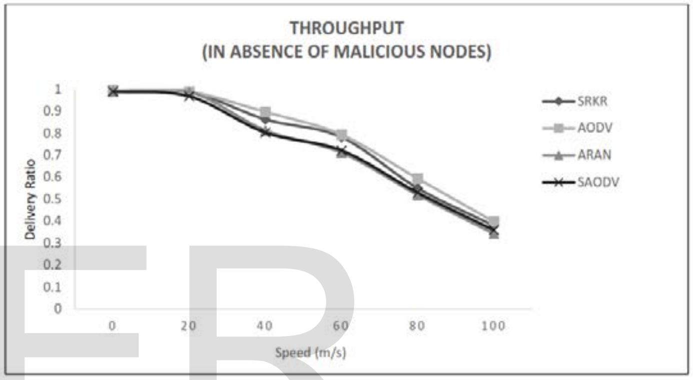

Fig:-1(A)- Throughput in the absence of Malicious Node

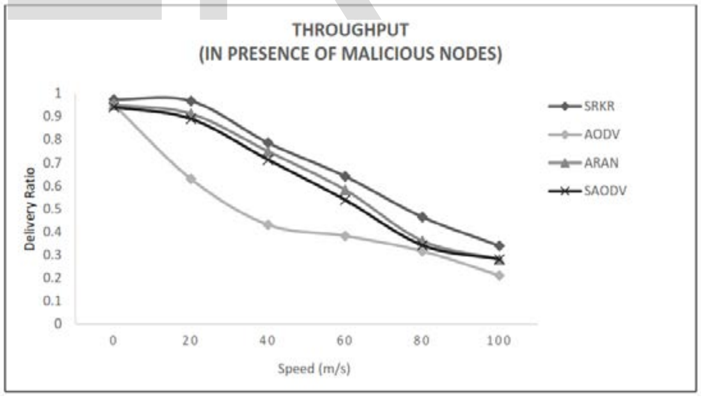

Fig:-1(B)- Throughput in the 40% presence of Malicious Node

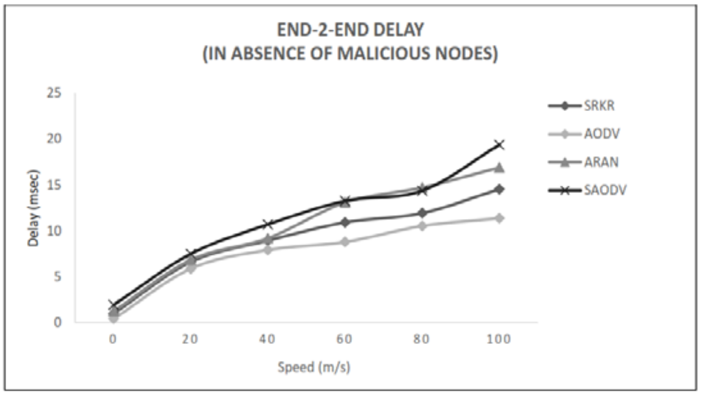

Fig:-2(A)- End-2-End Delay in the absence of Malicious Node

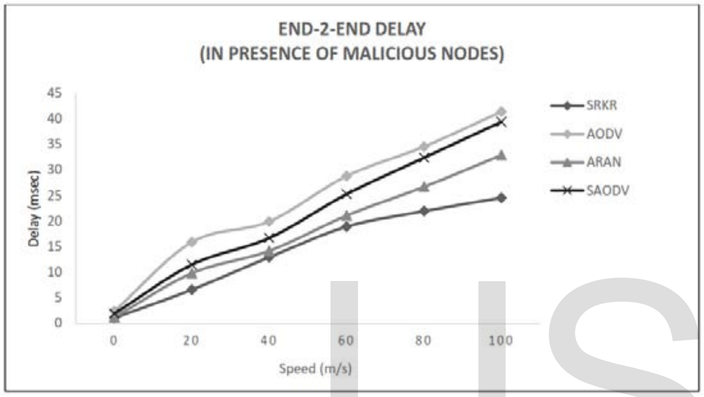

Fig:-2(B)- End-2-End Delay in the presence of Malicious Node

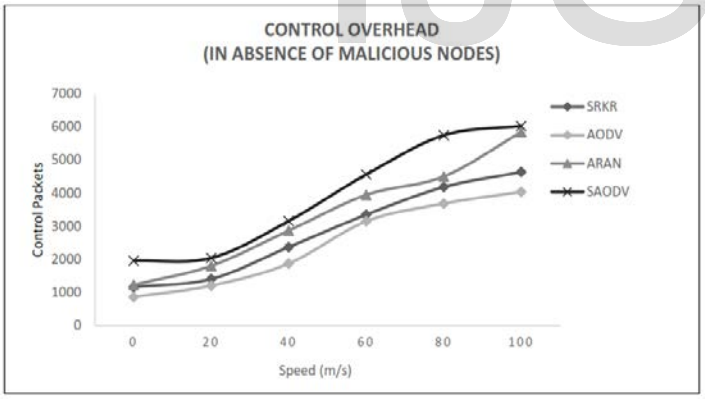

Fig:-3(A)- Control Overhead in the absence of Malicious Node

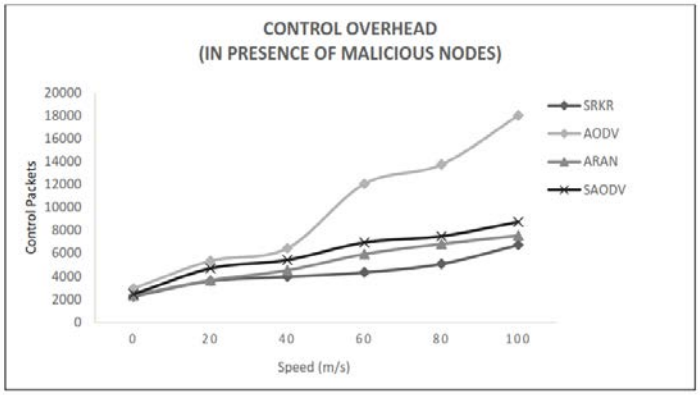

Fig:-3(B)- Control Overhead in the presence of Malicious Node

5 Conclusion

We presented secure reliable key routing (SRKR) protocol for mobile ad hoc network, which secure the routing mechanism from both internal and external attacks. It authenticates route discovery messages using public key cryptography and secure data routing packets using symmetric cryptography using unique session and secret key. The experimental evaluation of SRKR shows an improvisation in throughput and routing overhead in case of malicious presence in the network in compare with AODV, SAODVand ARAN. It provides a novel contribution in providing double shielding security to routing message and data packets makes attackers difficult for intrusion.

An enhancement to protocol can be made in future to evaluate more sensitive parameter of the protocol which can effects the cryptography process, and from simulation it was also observed that effects of mobility have high impact on the performance of mobile adhoc network, so one can enhance the protocol to handle link failure and repairing process in future work.

References

[1] R.Lacuesta,J.Lloret,M.Garcia,and L.Penalver, A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation, IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 4, April 2013

[2] I.Khalil and S.Bagchi, Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure IEEE Transactions On Mobile Computing, Vol. 10, No. 8, August 2011

[3] R.V.Boppana and Xu Su, On the Effectiveness of Monitoring for Intrusion Detection in Mobile Ad Hoc Networks. IEEE Transactions On Mobile Computing, Vol. 10, No. 8, August 2011

[4] V. Kumar and M.L. Das, "Securing Wireless Sensor Networks with Public Key Techniques," Ad Hoc and Sensor Wireless Networks, vol. 5, nos. 3/4, pp. 189-201, 2008.

[5] M.Guerrero Zapata and N.Asokan, "Securing Ad hoc Routing Protocols," in Proceedings of the 1st ACM workshop on Wireless security, Atlanta, GA, USA, Sep 2002, pp. 1-10.

[6] K.Sanzgiri,B.Dahill, B.N.Levine, C.Shields, and E.M.Royer. A Secure Routing Protocol for Ad Hoc Networks (pdf). Technical Report: UM-CS-2002-032, 2002.

[7] A.Pirzada,C.McDonald, Secure routing with the AODV protocol, Proc. the Asia-Pacific Conference on Communications, 2005, 57-61.

[8] [8]. D.B.Johnson, D.A.Maltz and Y.C.Hu. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). IETF INTERNET DRAFT, MANET working group, July. 2004.

[9] W. Yu, Y. Sun, and K.J.R. Liu, "HADOF: Defense against Routing Disruption in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2005.

[10] W. Yu, Y. Sun, and K.J.R. Liu, "Stimulating Cooperation and Defending against Attacks in Self-Organized Mobile Ad Hoc Networks," Proc. Second Ann. IEEE CS Conf. Sensor and Ad Hoc Comm. and Networks (SECON '05), 2005.

[11] K. Liu, J. Deng, P.K. Varshney, and K. Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Trans. Mobile Computing, vol. 6, no. 5, pp. 488-502, May 2007.

[12] C.E.Perkins, E.M.Royer, and S.R.Das. Ad Hoc On- Demand Distance Vector (AODV) Routing. IETF INTERNET DRAFT, MANET working group. Feb. 2003.

[13] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47, Feb. 2004.

[14] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-Securing Ad Hoc Wireless Networks," Proc. Seventh IEEE Symp. Computers and Comm. (ISCC '02), 2002.

[15] Abedi O,M. Fathy, Enhancing AODV routing protocol using mobility parameters in VANET, IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2008.

[16] P.Papadimitratos and Z.Haas. Secure routing for mobile ad hoc networks. In SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, 2002.

[17] N.Asokan and P.Ginzboorg, Key agreement in ad-hoc networks. Computer Communication Review, 23:1627-1637, 2000.

[18] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. Providing robust and ubiquitous security support for wireless mobile networks. In ICNP, pages 251-260, 2001.

[19] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks," Computer Comm., vol. 30, nos. 11/12, pp. 2314-2341, Sept. 2007.

[20] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: A Lightweight Hopby- Hop Authentication Protocol For Ad-Hoc Networks," Ad Hoc Networks J., vol. 4, no. 5, pp. 567-585, Sept. 2006.

[21] J. Yan, J. Ma, F. Li, and S.J. Moon, "Key Pre-distribution Scheme with Node Revocation for Wireless Sensor Networks," Ad Hoc and Sensor Wireless Networks, vol. 10, nos. 2/3, pp. 235-251, 2010.

[22] M. Mukesh and K.R. Rishi, "Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review," Int'l J. Computer Applications, vol. 12, no. 2, pp. 37-43, Dec. 2010.

[23] K. Sahadevaiah and P.V.G.D. Prasad Reddy, "Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks," Network Protocols and Algorithms, vol 3, no. 4, pp. 122-140, 2011.