

## International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

*IJCSMC, Vol. 4, Issue. 8, August 2015, pg.29 – 32*

### **RESEARCH ARTICLE**

# **SECURE BASED ROUTING PROTOCOL WITH CRYPTOGRAPHY DATA ENCRYPTION TECHNIQUE FOR MANET**

*S.Christy Sheeba<sup>1</sup>, V.Palanisamy<sup>2</sup>  
Mphil Research scholar<sup>1</sup>, Head of the Department<sup>2</sup>  
Department of Computer Science and Engineering  
Alagappa university, karaikudi, India  
Email: Sheebu05@gmail.com*

### **Abstract**

*Mobile Ad hoc Networks are deployed in many new domestic and public applications, rising to new requirements in terms of performance and efficiency. However due to their nature, some usual network services as routing and security are not carried out as well as expected. Securing routing protocols is one of these challenging tasks, since security is not natively implemented in ad hoc routing, and the extensions given in literature are complex and vulnerable against several attacks. Therefore in this paper we propose an implementation of Data and link security exploiting the route discovery and route reply mechanisms of proactive routing protocols to publish self-issued certificates in a distributed fashion. These certificates are used by mobile nodes to secure communications, ensure authentication, integrity, confidentiality and detect attacks in mobile ad hoc networks. Our proposed scheme is simple and utilizes the underlying protocol as a support for certificate publishing; therefore it does not affect the performance of the network.*

*Keywords: AES, Manet, security, NS2.*

### **1. Introduction**

Our routing protocol is based on Dynamic Source Routing (DSR) and Ad Hoc on Demand Distance Vector Routing (AODV) [1]. The route discovery process in DSR is almost similar to the AODV protocol, except that each intermediate node that broadcasts a route request (RREQ) packet adds its own address identifier to a list carried in the packet. The destination node generates a route reply (RREP) message that includes the list of addresses received in the route request and transmits it back along this reverse path to the source. The details of most related paper of our research work are given below. K.Sanzgiri and all; proposed secure routing protocol called ARAN, ARAN is a on-demand secure routing protocol [2]. It detects and protects against authentication, message integrity and non-repudiation. It uses asymmetric key cryptography. ARAN requires trusted certification server, The certificate accommodates the IP address of the node, its public key and a time-stamp of when the certificate was created and a time at which the certificate expires along with the signature by

certification authority. But the disadvantages of ARAN is it uses the central authority (Certification Authority) and it can't protect against worm hole attack. Adrian Perrig and all ; proposed secure routing protocol called ARIADNE, A secure on demand routing protocol for ad-hoc network (ARIADNE) is based on DSR routing protocol, it uses highly efficient symmetric cryptography [3]. It provides point-to-point authentication of a routing packets using a message authentication code (MAC) and a shared key between the two parties. For broadcasting RREQ packets it uses TESLA broadcast authentication protocol. TESLA keys are distributed to the participating nodes via an online key distribution center. Yih-Chun Hu and all; proposed secure routing protocol called SEAD, Secure Efficient Ad-Hoc Distance Vector (SEAD) is based on destination-sequenced distance vector routing (DSDV) protocol [4].It is a proactive routing protocol. SEAD deals with attackers that modify routing information broadcast during the update phase of the routing information. SEAD makes use of efficient one-way hash chains rather than relying on expensive asymmetric cryptography operations. SEAD does not cope with wormhole attacks. K.Sanzgiri and all; proposed routing protocol called A Secure Routing Protocol for Ad hoc Networks (SRP), relies on the availability of a security association (SA) between the source node and the destination node [5]. The SA could be established using a hybrid key distribution based on the public keys of the communicating parties. Source and destination can exchange secret key using each others public key [6]. Manel Guerrero Zapata; proposed a routing protocol called Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing, it is a extension of AODV protocol [7]. The Secure AODV scheme is based on the assumption that each node possesses certified public keys of all network nodes. SAODV can be used to protect the route discovery mechanism of the AODV by providing security features like integrity, authentication and non repudiation. But in ad hoc network each node will know the others public key its a challenge. Seung Yi and all; proposed a secure routing protocol called Security-Aware Ad-Hoc Routing (SAR). SAR is the generalized framework for any on demand ad-hoc routing protocol. SAR uses Key distribution or secret sharing mechanism. SAR may fail to find the route if the ad hoc network does not have a path on which all nodes on the path satisfy the security requirements in spite of being connected. Panagiotis Papadimitratos and all; proposed secure routing protocol called Secure Link State Routing Protocol (SLSP) [8]. To function effectively without central key management authority, SLSP enables each node to periodically broadcast its public key to nodes within its zone. To achieve theses goals a Neighbor Lookup Protocol (NLP) is made an integral part of SLSP. Ranga Ramanujan and all; proposed a secure routing

protocol called Techniques for Intrusion-Resistant Ad Hoc Routing Algorithms (TIARA) [9]. TIARA mechanisms protect ad hoc networks against denial-of-service (DoS) attacks launched by malicious intruders. TIARA addresses two types of attacks on data traffic which are flow disruption and resource depletion. It requires online public key infrastructure. Srdjan Capkun and all; proposed secure routing protocol called Building Secure Routing out of an Incomplete Set of Security Associations (BISS). The sender and The receiver can establish a secure route, even if, prior to the route discovery, only the receiver has security associations established with all the nodes on the chosen route. It signs the request with its private key and includes its public key PKI in the request along with a certificate signed by the central authority binding its id with PKI. Frank Kargl and all; proposed secure routing protocol called Secure Dynamic Source Routing (SDSR) Protocol. It is based on DSR routing protocol. It checks the mutable and immutable field of the routing packets. and secure the authenticity of all nodes participating in a route . A Sivakumar Kulasekaran and all; proposed a secure routing protocol called An efficient secure route discovery protocol for DSR. It uses the peer review process to make to secure routing protocol secure but it uses only DSR routing protocol, packet size of the DSR routing protocol increase on passing by the intermediate nodes. Phung Huu Phu and all; proposed a secure routing protocol called securing AODV routing protocol in MANET. In this paper, each node tries to establish key exchange in with its neighbour but if any node provides any wrong information then it has to rely on it [9]. Calinescu Gruia; proposed a scheme to compute the two hop distance node in "Computing 2-Hop Neighborhoods in Ad Hoc Wireless Networks", it has been shown that a node can find out its two hop neighbour safe and securely. Bathini Eswar and all; uses two hop distance node to improve AODV Routing protocol [10].

In MANET there are different kinds of protocol types are used, here we will see reactive and proactive protocols.

## **2.SRAP Mechanism:**

Our main focuses are to introduce SRAP to protect data transmission and to construct a secure routing protocol.

our SRAP approach uses a Mobile of security mechanisms so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route. The security mechanisms that the protocol uses are the hash function, Certificates, time synchronization and route discovery request. SRAP

works as a group and has Four stages, examined in turn in the remainder of this section:

#### 2.1 Route Request Process:

1. Route Request message MD5 encryption by Destination
2. Send Encrypted Route Request Message with Symmetric key from Destination with unique ID (MAC Address)
3. Decrypting MD5 by source and check the route request

#### 2.2 Detect and Eliminate the Attackers from The Routing table Process:

4. Detecting Attackers in the network by looking up duplicate requests
5. Removing those nodes from the routing table

Certificate Distribution to all the authenticated nodes:

6. Source Generates and distribute the Certificates to all the authenticated nodes

#### 2.3 Packet Transfer Process:

7. Sending Packets to the proper destination with SES data encryption technique
8. Receiving packets and SES decryption by destination

#### 2.4 Route Request Process:

The MD5 hash function is used to encrypt and update the Request data necessary for the routing process in order to secure the mutable data request, which in this case is the head direction and time to find a proper unique destination, whose information uses hash chains. SRAP uses hash chains in order to secure the mutable data request of the head direction and Td, the maximum time to find a destination node, for any node in the network, including an intermediate node and the destination node, which when it receives the message can verify that the mutable data request has not been decremented by any attacker. SRAP forms a hash chain by applying it one way. A hash function is the operation whereby a node creates an RREQ and a hash function repeatedly to begin. The MD5 Hash function functionality is explained briefly in next headings. Using these Request packets is being encrypted and sending to the source. The source node will have the symmetric key to decrypt this message to read the proper request message.

#### 2.5 Detect and Eliminate the Attackers from The Routing table Process:

Using the above process source node could easily find the proper destination. And it could easily find the attackers by receiving duplicate requests. It would be the strongest way to find the attackers and eliminate from the network by removing these from routing table.

#### 2.6 Certificate Distribution to all the authenticated nodes:

SRAP adopts the Source node generate Certificate approach because of its superiority in distributing keys and achieving integrity and non-repudiation. The system uses symmetric and public keys. The symmetric key is used to sign the certificate and the public key of all the nodes, while the public key is used to renew certificates that are issued by source node. All nodes must to have verified certificates. The public keys and the corresponding symmetric keys of all nodes are created by the source node, which also issue the public-key certificates of all nodes. Each node has its own public/Symmetric key pair. Public keys can be distributed to another node in the secure path stage, while Symmetric keys should be kept confidential to individual nodes.

Each node in SRAP approach receives exactly one certificate after securely authenticating its identity to the Source. Each node will hold its certificate in the Node Databases. The main structure of node certificates, it contains the identifier of the node, its public key, the name of the source issuing this certificate, the certificate issue and expiry dates, and the public key of the node. Finally, the contents of the certificate will be attached to the signature of the source node. All nodes in a network should maintain fresh certificates with the source node. At the secure path stage, nodes use their certificates to authenticate themselves to other nodes in the network.

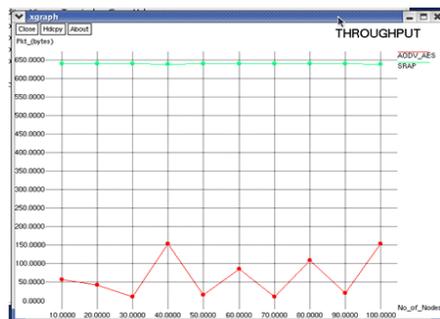
#### 2.7 Packet Transfer Process:

SRAP approach is to use a SES algorithm to establish secure data between nodes. The Secure Path Stage is found in the first process and is based on the requirement for all nodes to have a secure path with other nodes before sending any route request packet. Any node receiving an RREQ from the source node or another node without a secure path should discard the request. In our approach, each node is given the system public key in order for any node to be able to send a Secure Path Request to another node the first time the certified public keys are exchanged. The authenticity of the certificate can be confirmed as the nodes have the system public key. The first objective of the SPS is the exchange of the

certified public keys and their confirmation, while its second objective is to ensure the identity of the sender before acceptance of the RREQ. The SPS considers secure authentication node by node.

### 3.Result:

The performance data of four routing protocols (AODV and SRAP) are collected. A scenario is set up for data collection. This scenario is run 10 times with 10 different values of the mobility ranging from 10 to 100 seconds. In general, the actual values of the performance metrics in a given scenario are affected by many factors, such as node speed, moving direction of the nodes, the destination of the traffic, data flow, congestion at a specific node, etc. It is therefore difficult to evaluate the performance of a protocol by directly comparing the acquired metrics from individual scenarios. In order to obtain representative values for the performance metrics, we decided to take the average values of multiple simulation runs. The average values of these 10 simulation runs are then calculated for the two metrics and used as a baseline to evaluate the performance of routing protocols in malicious environments.



Simulation Result of Node Vs Throughput

### 4.CONCLUSION

we proposed the security mechanism SRAP to routing protocols should prevent external attacks, including black holes and routing holes, while providing viability, confidentiality and authentication. Time synchronization is used to provide the protocol with the ability to find the route and to ensure that the selected route is the correct path. The digital signature mechanism, when applied to routing protocols, should prevent internal attacks, including impersonation, and should provide non-reputation and integrity

The solution is a combination of the history of the nodes and operation certificates. Each node in a secure environment is uniquely identified by its public key, Symmetric key and MAC address. The solution addresses various vulnerability issues affecting wireless

links such as active and passive attacks. The dynamic nature of networks and their membership does not affect the solution, since each node makes access decisions on its own and the use of cooperative algorithms is avoided. We have compared SRAP with AODV protocol and proved that our SRAP is more better than all other protocols and increased the security level from 75% to 86%.

### 5.REFERENCES:

- [1] Mourad Elhadef, Azzedine Boukerche, and Hisham Elkadiki. Diagnosing mobile ad-hoc networks: two distributed comparison-based self-diagnosis protocols. In Proceedings of the 4th ACM international workshop on Mobility management and wireless access, pages 18–27. ACM, 2006.
- [2] George Aggelou. Mobile Ad Hoc Networks. Tata McGraw-Hill, 2009.
- [3] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester. An overview of mobile ad hoc networks: Applications and challenges. JOURNAL-COMMUNICATIONS NETWORK, 3(3):60–66, 2004.
- [4] Humayun Bakht. Applications of mobile ad-hoc networks. <http://www.computingunplugged.com/issues/issue2004-09/00001371001.html>, 2004.
- [5] Samba Sesay, Zongkai Yang, and Jianhua He. A survey on mobile ad hoc wireless network. Information Technology Journal, 3(2):168–175, 2004.
- [6] Imrich Chlamtac, Marco Conti, and Jennifer J-N Liu. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, 1(1):13–64, 2003.
- [7] Sudhir Agrawal, Sanjeev Jain, and Sanjeev Sharma. A survey of routing attacks and security measures in mobile ad-hoc networks. arXiv preprint arXiv:1105.5623, 2011.
- [8] POWAH YAU, Shenglan Hu, and Chris J Mitchell. Malicious attacks on ad hoc network routing protocols. Information Security Group.
- [9] Djamel Djenouri, L Khelladi, and N Badache. A survey of security issues in mobile ad hoc networks. IEEE communications surveys, 7(4), 2005.
- [10] Petteri Kuosmanen. Classification of ad hoc routing protocols. Finnish Defence Forces, Naval Academy, Finland, petteri.kuosmanen@mil.fi, 2002.