Volume 2, Issue 5, May 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Implementing Authentication Mechanism using Extended Public Key Cryptography in Wireless Network

Sandip A. Kahate[1#],
[1]*ME Student, Dept of CSE,*
G.H. Raisoni College of Engineering,
Nagpur (MS) INDIA
[1#]sandip.kahate@gmail.com

Kapil N. Hande[2#]
[2]*Assistant Professor, Dept of CSE,*
G.H. Raisoni College of Engineering,
Nagpur (MS) INDIA

Abstract- ***Mobile ad hoc network is a special kind of wireless networks. 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. The proposed mechanism will authenticate the node and ensure the security of important routing information in AODV protocol.***

Keywords: MANET Security, AODV Routing Protocol, ns-2, Extended public key, Hybrid Cryptography

I. INTRODUCTION

Wireless cellular system has been in use since 1980s. Wireless system operates with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to other. In wireless system the device communicate via radio channel to share resource and information between devices. Due to presence of a fixed supporting structure, limits the adaptability of wireless system, so this generation of wireless system is required easy and quick deployment of wireless network. Recent advancement of wireless technologies like Bluetooth. Introduced a new type of wireless system known as Mobile ad-hoc network (MANETs) [1], which operate in the absence of central access point.

It provides high mobility and device portability's that enable to node connect network and communicate to each other. It allows the devices to maintain connections to the network as well as easily adding and removing devices in the network. User has great flexibility to design such a network at cheapest cost and minimum time.

Mobile ad hoc network consist large number of node, it form temporary network with dynamic topology. In this network each node communicates with each other through radio channel without any central authority. In MANETs each node operates in a distributed peer-to- peer modes, serves as an independent router to forward message sent by other nodes.

MANETs has shows distinct characteristics, such as:

- Weaker in Security
- Device size limitation
- Battery life
- Dynamic topology
- Bandwidth and slower data transfer rate

Apart from these limitation MANETs has many extensive application like: Military application, Natural disaster, Medical service. In ad hoc network there can be node that will try to disrupt the proper functioning network. These nodes can be malicious or selfish. They try to disrupt network function by modifying packets, injecting packets or creating routing loops. So, security is an important task, because MANETs has characteristics such as; dynamic topology, infrastructure less. There are large numbers of secure routing protocols proposed by many researchers they fulfill different security requirements and prevent specific attacks. They are divided into three categories: Reactive routing protocol [5, 6], Proactive routing protocol [5] and hybrid routing protocol [6].

In reactive routing protocol the route is discovered when it required, in proactive each node maintain network information regarding to network connectivity and route information to all others node within the network and proactive is one which is neither reactive nor proactive.

Now, the Most of the solution uses cryptography mechanism to detect selfish, malicious behavior of nodes and securing information from other types of attacks. The mechanisms which are used by different secure routing protocol to detect malicious and selfish node have address separately in different protocol. No secure mechanism has been proposed till date that can address to detecting malicious and selfish node collectively. We proposed a mechanism, Extended Public key Cryptography (EPKCH) [12] that able to detect the malicious nodes and selfish nodes collectively in order to achieving security goals such as; Authentication, Integrity, Confidentiality. Also, we proposed a routing protocol named Authenticate and Secure Routing protocol for mobile Ad hoc Network (AMSRP). We implemented EPKCH mechanism in monitor mode of AMSRP to securing MANETs. To design of this protocol follows the table-driven approach, in which each node maintain the information, regarding to network structure and route from a particular source to its all possible destination in its node info table. AMSRP is a reactive secure routing protocol.

II. LITERATURE REVIEW

The problem of security of various malicious attacks on network area has received considerable attention by researchers in the mobile ad-hoc network field. In this section, we discuss some of these works. Mechanisms for securing the routing layer of a MANET are proposed by [1]. Schemes to handle authentication in ad hoc networks by trusted certificates authorities (CAs) have been proposed by Zhou and Haas [2]. Four representative routing protocols are chosen for analysis and evaluation including: Ad Hoc on demand Distance Vector routing (AODV), Dynamic Source Routing (DSR),Optimized Link State Routing (OLSR) and Temporally Ordered Routing Algorithm (TORA). Secure ad hoc networks have to meet fivesecurityrequirements:confidentiality,integrity,authentication,non-repudiation and availability. The analyses of the secure versions of the proposed protocols are discussed with respect to the above security requirements by *Loay Abusalah, Ashfaq Khokhar[3]*.

In an *ad hoc network*, mobile computers (or nodes) cooperate to forward packets for each other, allowing nodes to communicate beyond their direct wireless transmission range. Many proposed routing protocols for ad hoc networks operate in an *on-demand* fashion, as on-demand routing protocols have been shown to often have lower overhead and faster reaction time than other types of routing based on periodic (proactive) mechanisms. Significant attention recently has been devoted to developing secure routing protocols for ad hoc networks, including a number of secure on demand routing protocols, that defend against a variety of possible attacks on network routing. denial-of-service when used against *all* previous on-demand ad hoc network routing protocols. For example, DSR, AODV, and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack. This attack is also particularly damaging because it can be performed by a relatively weak attacker. We analyze why previous protocols fail under this attack. We then develop *Authentication Mechanism Secure Routing Protocol(AMSRP)*.

Some researchers have also focused on finding and reporting misleading routing misbehavior of nodes using different technique. *Shashi Mehrotra Seth, Rajan Mishra* compare AES and RSA algorithms for data communication consume a significant amount of computing resources such as CPU time, memory and battery power and computation time. AES and RSA considering certain parameters such as computation time, memory usages and output byte[10] But we are design the new security protocol using hybrid encryption technique for securing misbehavior and malicious nodes. The hybrid encryption technique is a combination of both symmetric and asymmetric cryptographic techniques. The encryption algorithms are more secured depends on the key value and its size. But, the key distribution is major problem. The various protocols are currently given the solution. The new protocol solves the key management problem using key servers. It also provides all the three cryptographic primitives - integrity, confidentiality and authentication. In this proposed design methodology, the new protocol design using Symmetric cipher (AES-Rijndael) for encryption /decryption process and MD5 pure algorithm and RSA extended public key cryptography for integrity and authentication[13,14]

III. SECURITY PROBLEM WITH EXISTING AD HOC ROUTING PROTOCOLS

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.

IV IMPLEMENTATION

Module Implementation Status

a) Phase1: Performance Analysis of AODV
b) Phase2: AES Implementation Module
c) Phase3: RSA & MD5 Implementation Module

a) Phase 1: Performance Analysis of AODV (Route Discovery & Maintenance)

• *Route Request Message RREQ:*

Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

• *Route Reply Message RREP:*

A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

• *Route Error Message RERR:*

Every node in the network keeps monitoring the link status to its neighbor's nodes during active routes. When the node detects a link crack in an active route, Route error (RERR) message is generated by the node in order to notify other nodes that the link is down.

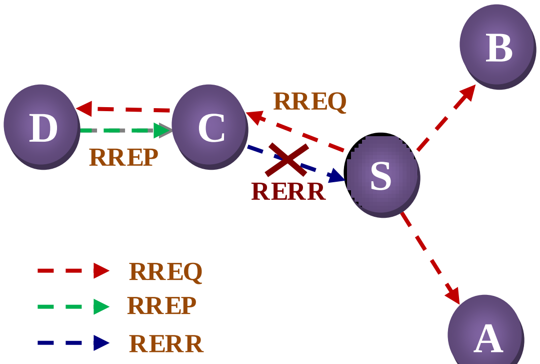


Fig.1 Route Maintenance

•*Route Discovery in AODV:*

- A source node S wishes to communicate with destination node D broadcast a Route Request (RREQ) to its neighbors
- Intermediate nodes forward the RREQ to their neighbors
- The destination node sends a Route Reply Message (RREP) back to the source node
- An intermediate node may send a RREP provided that it knows a 'fresh enough' route to the destination
- Nodes maintain routing table entries only for active routes, unused routes are removed from the routing table after *active_route_timeout* interval

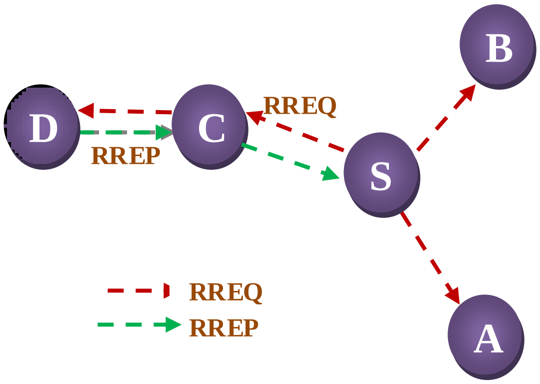


Fig.2 Route Discovery

b) Phase 2: AES Implementation Module

This standard specifies the Rijndael algorithm a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits.Mathematical properties that are useful in understanding the algorithm. Algorithm specification, covering the key expansion, encryption, and decryption routines; Implementation issues, such as key length support, keying restrictions, and additional block/key/round sizes.The algorithm was designed to have the following characteristics:

• Resistance against all known attacks

• Speed and code compactness on a wide range of platforms

• Design simplicity

• Input to the encryption algorithm, decryption algorithm in a single 128 bit block

In AES, four different stages are used

1. Substitution bytes

Use S-box to perform byte-to-byte substitution of the block

2. Shift rows

A simple permutation

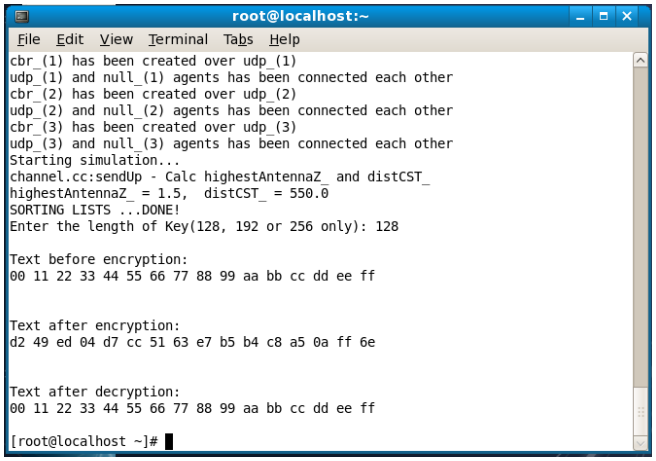
3. Mix columns

A substitution that makes use of arithmetic

4. Add round key

A simple bit wise XOR of the current block with the portion of the expanded key

In add round key stage makes use of the key. Any other stage applied at the beginning or end is reversible without knowledge of the key, this scheme is more efficient and secure.



```
cbr_(1) has been created over udp_(1)
udp_(1) and null_(1) agents has been connected each other
cbr_(2) has been created over udp_(2)
udp_(2) and null_(2) agents has been connected each other
cbr_(3) has been created over udp_(3)
udp_(3) and null_(3) agents has been connected each other
Starting simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
Enter the length of Key(128, 192 or 256 only): 128

Text before encryption:
00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff


Text after encryption:
d2 49 ed 04 d7 cc 51 63 e7 b5 b4 c8 a5 0a ff 6e


Text after decryption:
00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff

[root@localhost ~]#
```

Fig.3 Screenshot of AES Encryption & Decryption Process using length of key 128 in NS2

c) Phase 3: RSA & MD5 Implementation Module

i) RSA Algorithm

The RSA algorithm uses two keys, *d* and *e*, which work in pairs, for decryption and encryption, respectively.

- A plaintext message P is encrypted to cipher text by: $C = Pe \bmod n$
- The plaintext is recovered by: $P = Cd \bmod n$
- Because of symmetry in modular arithmetic, encryption and decryption are mutual inverses and commutative. Therefore,

  $P = Cd \bmod n = (Pe)d \bmod n = (Pd)e \bmod n$
- Thus, one can apply the encrypting transformation first and then the decrypting one, or the decrypting transformation first followed by the encrypting

ii) RSA & MD5 Implementation Module:

- MD5 algorithm can be used as a digital signature mechanism.

- This presentation will explore the technical aspects of the MD5 algorithm.
- Takes as input a message of arbitrary length and produces as output a 128 bit "message digest" of the input.
- It is computationally infeasible to produce two messages having the same message digest.
- Intended where a large file must be "compressed" in a secure manner before being encrypted with a private key under a public-key cryptosystem such as RSA

V. PROPOSED IMPLEMENTATION WORK

This proposed mechanism presents a secure communication between the mobile nodes using Hybrid cryptography. A scenario of data transmission between the two mobile nodes has been considered. Whenever a source wants to transmit the data packets to the destination, it ensures that the source is communicating with real node. The authentication service uses a key management to retrieve the extended public key, which is trusted by the third party for identification of the destination. The destination also used similar method to authenticate the source. After execution of the key management module, a shared key is invoked; this is used by both source and destination for further communication confidentially. In this way, all the important messages are transmitted to the destination.

In this hybrid encryption approach, sender side using 128-bit session key value with AES-Rijndael to encrypt the message. The hash value of message was encrypted using RSA algorithm with 1028 bit Extended Public key of the receiver. In the receiver side the decryption done for the encrypted message using AES-Rijndael with 128-bit session key value.

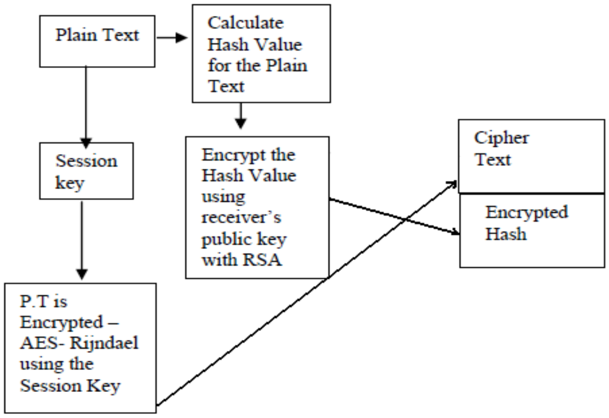

Plain Text
Calculate Hash Value for the Plain Text
Session key
Encrypt the Hash Value using receiver's public key with RSA
Cipher Text
Encrypted Hash
P.T is Encrypted – AES- Rijndael using the Session Key

Fig. 4 Encryption Process & Authentication

To calculate the hash value using hash function MD5 for the original message. Using RSA with 1028 bit extended private key of the receiver to decrypt the encrypted hash value. To ensure the integrity the comparison performed between calculated and decrypted hash values. The following figure 2 and figure 3 explain this process.

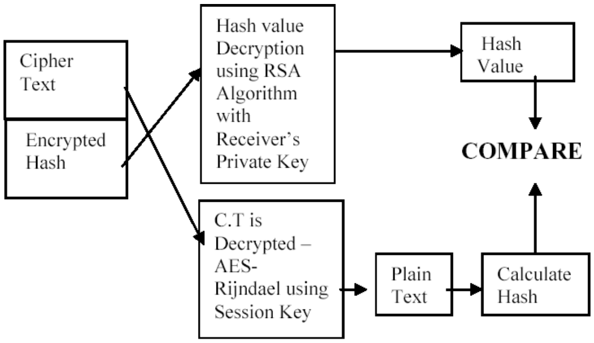

Cipher Text
Encrypted Hash
Hash value Decryption using RSA Algorithm with Receiver's Private Key
Hash Value
COMPARE
C.T is Decrypted – AES- Rijndael using Session Key
Plain Text
Calculate Hash

Fig. 5 Decryption Process & Authentication

VI. IMPLEMENTATION AUTHENTICATION SECURITY IN WIRELESS NETWORK

A) Algorithm

Step 1: The public key and private key for each node is generated using RSA algorithm

Step 2: After generating private key and public keys, the source (S) and destination (D) performs public key exchange using its own private key

Step 3: encryption of message at S and decryption by D occurs.

Step 4: Once the sender starts its transmission, each node will generate its own certificate using MD5 pure algorithm

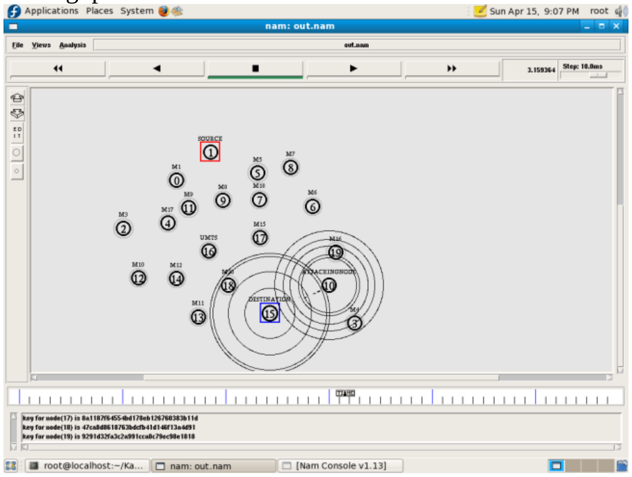
Step 5: The neighbor node will check the certificate and after making verification, it will deliver the packet meant for destination

Step 6: If any node which is not a member of this transmission process tries to get the packet by issuing a certificate,

Step 7: the node may be considered as an intruder and the certificate will be considered as a bad certificate.

Routing is done with *Authentication Mechanism Secure Routing Protocol(AMSRP)* using AODV protocol. Encryption and Decryption by AES Algorithm. Certificate generation is by MD5 pure Algorithm for integrity and Authentication provided by RSA.

Initially all the nodes are fully energized. It prepares to start its transmission. The red shade square indicates that a node has source node(Node 1) i.e. active mode. The blue shade square indicates that it has gone for destination node(Node 15). The source starts its transmission in active mode and then to destination node. The recipient after getting the message goes to destination node in order to transmission packets. The next state is , some nodes may go into weak state which is shown by an yellow shade as each node may spent its energy by encrypting and decrypting and in certificate checking by CA node (Node 3). But the malicious node (node 10) which is with full energy level may try to interpret the message from the destination. Now, the malicious node (node 10) enters into the zone and tries to intercept the message from its nearest destination and sends a fake certificate to active neighboring nodes.. As the node finds it, the malicious node's request gets rejected. So some of the energy is spent and so, to retain its remaining energy, the node again moves to Before the time scale comes to an end, many nodes go to sleep state as they get exhausted in certificate checking and verifying. The figure 6 show the simulation scenario of the nodes. This process affirms an end-to-end authentication security for the entire period of transmission. As the security feature is much concentrated, it minimize some delay and increases throughput.



```
key for node(17) is 8a1187f6455 4bd178eb126760383b11d
key for node(18) is 47ca8d8618763bdcfb41d146f13a4d91
key for node(19) is 9291d32fa3c2a991cca8c79ec98e1818
```

Fig.6 Simulation Scenario of Packets Delivery nodes

VII. CONCLUSION & FUTURE WORK

There are various MANET protocols proposed by the subject to a variety of attacks through the modifications or fabrications of routing message or impersonations of other nodes. It allows the attackers to influence the victim's selection of routes or enable the denial of service attacks. In this mechanism, we have implements the security issues for MANETs. It focuses on the authentication security architecture. As a part of future work we will analysis experimental performance result of implement mechanism.

REFERENCES

[1] Rachika Gupta (2011) Mobile adhoc network(MANETS):Proposed solution to security related issues, Indian J. Computer Science and Engineering (IJCSE) 2(5):748-46

[2] Papadimitratos P,Haas Zhou (2002) Secure routing for mobile ad hoc networks, In Proceedings of SCS Communications Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX.

[3] Loay Abusalah,Ashfaq Khokhar, Mohsen Guizan (2008) A Survey of secure mobile ad hoc routing protocols. IEEE Communications Surveys & Tutorials, 10(4):78-93

[4] Yih ChunHu, Adrian Perrig, David B Johnson (20030 Rushing Attacks and Defense in Wireless Ad Hoc NetworkRouting Protocols, WiSe San Diego, California, USA. Copyright 2003 ACM 1581137699/ 03/0009.

[5] Panagiotis Papadimitratos, Zygmunt J Haas (2002) Secure Routing for Mobile Ad hoc Networks, In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX.

[6] Syed S Rizvi (2010) Combining private and public key encryption techniques for providing extreme secure environment for an academic institution application. Int. J. Network Security & Its Application (IJNSA), 2(1)2010.

[7] Padmavathi G (2010) CCMP-AES model with DSR routing protocol tosecure Link layer and network layer in Mobile adhoc networks.Int. J. Computer Science and Engineering 2(5):1524-31

[8] Matin MA, Hossain MM, Hossain MFI (2010) Performance Evaluation of Symmetric Encryption Algorithm in MANET and WLAN, IEEE Xplore.

[9] Emmanouil A Panaousis, George Drew, Grant P Millar, Tipu A. Ramrekha (2010) A test-bed implementation for securing olsr in mobile ad-hoc networks. Int. J. Network Security & Its Applications 2, (4) 2412 -143

[10] Monis Akhlaq, M Noman Jafri (2006) Addressing Security Concerns of Data Exchange in AODV Protocol, World Academy of Science, Engineering and Technology.

[11] Seth SM, Mishra R (2011) Comparative analysis of encryption algorithms for data communication 2(2): 102-103.

[12] Ramaraj E, Karthikeyan S, Hemalatha M A Design of Security Protocol using Hybrid Encryption Technique (AES- Rijndael and RSA*)"*

[13] B. Sreedevi *S. Ramanujan, Centre, Sastra University, Kumbakonam,* Y. Venkatramani, *Saranathan College of Engineering, Trichy. India* T. R. Sivaramakrishnan*Sastra University, Thanjavur, India* "Implementing End-To-End Reliability and Energy Conservation Routing to Provide Quality of Service in Mobile Ad hoc Networks" European Journal of

Scientific Research ISSN 1450-216X Vol.55 No.1 (2011), pp.28-36

[14] S. Subasree and N. K. Sakthivel," Design of a new Security Protocol Using Hybrid Cryptography Algorithms" IJRRAS 2 (2) February 2010