INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

Implementing RSA Algorithm in MANET and Comparison with RSA Digital Signature

Spinder Kaur[1], Harpreet Kaur[2]

[1]Research Scholar, Department of Computer Science, Doaba Group of Colleges, Kharar, Punjab, India
spinder.kaur123@gmail.com
[2] Assistant Professor, Doaba Group of Colleges, ECE Department, Kharar, Punjab, India
tiwana_harpreeta @yahoo.com

Abstract: *Mobile ad hoc networks (MANETs) are collections of wireless mobile devices with restricted broadcast range and resources, and no fixed infrastructure. Communication is achieved by relaying data along appropriate routes that are dynamically discovered and maintained through collaboration between the nodes. Discovery of such routes is a major task, both from efficiency and security points of view. MANET is a self-configurable and self-determining network, and consists of various independent nodes. Securing MANETs is still an active area of research. In this paper, we are going to reduce the complexity of RSA algorithm and then we will implement this algorithm in Mobile ad-hoc networks (MANET). After implementing RSA algorithm using AODV protocol we will compare the performance of modified AODV protocol with RSA Digital Signature.*

Keywords: *MANET (mobile ad hoc network), RSA, AODV, DSR, Energy level.*

1. INTRODUCTION

Mobile Ad Hoc Network (also called MANET) MANETs are self-determining, self-maintained, and self-healing, allowing for external network flexibility. It is a network of mobile routers connected by wireless links - the union of which forms a unplanned topology. The routers are free to move randomly and organize themselves at random; thus, the network's wireless topology would change rapidly and uncertain. This type of network may operate in a standalone way, or would be connected to the larger Internet. Nodes in these networks will both generate user and application traffic and carry out network control and routing protocols. Rapidly changing connectivity, network allotments, maximum error rates, collision conflicts, and bandwidth and power constraints together pose new problems in network control—particularly in the design of higher level protocols such as routing and in implementing applications with Quality of Service requirements. Mobile applications present additional challenges for mesh networks as changes to the network topology are swift and widespread [1]. In a mobile ad hoc network, nodes move readily; therefore the network may experience rapid and unpredictable topology changes. Because the nodes in a MANET normally have limited range of transmission, some nodes cannot communicate directly with each other. Hence, routing tracks in mobile ad hoc networks potentially contain numerous hops, and every node in mobile ad hoc networks has the responsibility to perform like a router. Unlike devices in traditional Wireless LAN solutions, all nodes are mobile and the topology of the network is changing dynamically in an Ad Hoc Networks, which brings big and great challenges to the security of Ad Hoc Networks.[2][7]

2. CHARACTERSTICS OF MANET'S

a) In MANET, every single node acts as both host and router. That is it is self-determining in behavior.
b) Multi-hop radio relaying- When a server node and desired node for a message out of the radio range, the MANETs are suitable of multi-hop routing.
c) Distributed nature of operation for securing network, routing and host configuration. A centralized firewall is not available here.
d) The nodes can create or destroy the network anytime and making the topology dynamic in behavior.
e) Mobile nodes are characterized with few memory, power and light weight nature.
f) The reliability, efficiency, stability and capacity of wireless links are often lesser when compared with wired links. This

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

represents the fluctuating link bandwidth of wireless nodes.

g) Mobile and spontaneous nature which requires less human intervention to make up the network.
h) Higher user density and larger level of user mobility.
i) Nodal connectivity is periodic.[3][6]

3. ISSUES AND DIFFICULTIES

a) There is no centralized administration control, so it is difficult to find the paths between nodes.
b) Unprotected wireless channel.
c) Various types of transmissions and receiving lead to asymmetric nodes.
d) Scalability is one of the issues in the placement of nodes.
e) Selfish nodes decrease the performance.[4-5]

4. LITRATURE SURVEY

Mobile Ad hoc Network (MANET) technology is spreading widely these days because of its independence from fixed infrastructure. For MANET, acquiring highly finite resources, Symmetric key algorithms are more experienced and viable as compared to asymmetric key algorithms while transmitting messages via network due to less power consumption. Due to technological updating MANET is getting more and more accessible to common man, but the most important challenge that MANET is facing is the security issue. In this paper we described an enlarged approach of selective encryption algorithm for achieving better data protection. First we are giving an idea of selective encryption algorithm, and supposing an enhanced selective encryption algorithm based on symmetric key. By implementing the supposed method, the process of message encryption can be made more uncertain and limitations may be less, thereby making the encryption method more efficient. We will implement a set of simulation experiments on ns2 simulator in future to validate our proposed method [8].

With the proliferation of smart devices such as PDAs, smart phones and tablets in which having WIFI capabilities, applications coordinate massive mobile ad-hoc networks (MANETs) are under active development. These networks will have the potential of running communications without the use of pre-existing infrastructure, helps in the reduction of cost to carriers, creating communication networks where no infrastructure is present etc. For such utilities to be broadcast, they must take into account the security of data transferred within that network.

In this paper we explained an algorithm that will provide a secure key exchange during conversation hand-shake, on which a secure channel can be created. The algorithm assumes no previous knowledge and no user interposition, by using the inherent fluctuation of network topology in MANETs to allow for the discovery of an eavesdropper (if one exists). In this paper we proposed an algorithm, SDH that allows for secure key exchange with zero prior knowledge between sender and receiver.

Shortcomings: There is one major deficiency with SDH that must be further looked into. SDH, just like DH, does not take care of authentication. This implies that one does not know who he really is talking to. We assumed that the network addresses cannot be spoofed, and network routing cannot be influenced. This is true for most part, since routing information is widespread and constantly being updated by all around. Thus, the probability of being able to taint everyone's information all of the time is small. But theoretically speaking, if an attacker were able to do that, the SDH does not provide authenticity. It would be possible for the key exchange to be conducted with a different partner than was intended. To achieve authentication of parties as well, we must incorporate mechanisms that will operate above the actual connection. We leave that to further research [9].

5. OUR PROPOSED METHODOLOGY

In our proposed methodology we perform the following steps:

STEP-1 NETWORK FORMATION

Mobile nodes come closer to each other to form a temporary network. Any node can join or leave the network any time.

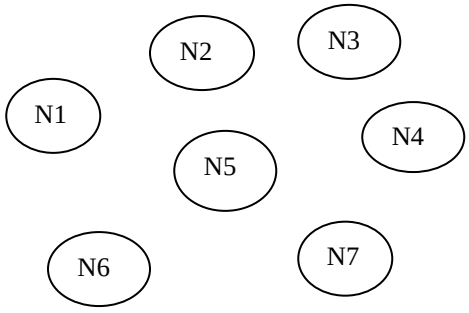

Figure 1: Mobile Nodes

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

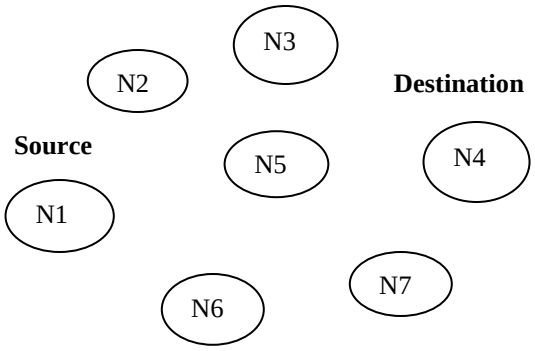

Figure 2: Path Selection

RSA is a cryptosystem, which is known as one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring product of two large prime numbers, the factoring problem.

- Choose two distinct prime numbers p and q.
- For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primarily test.

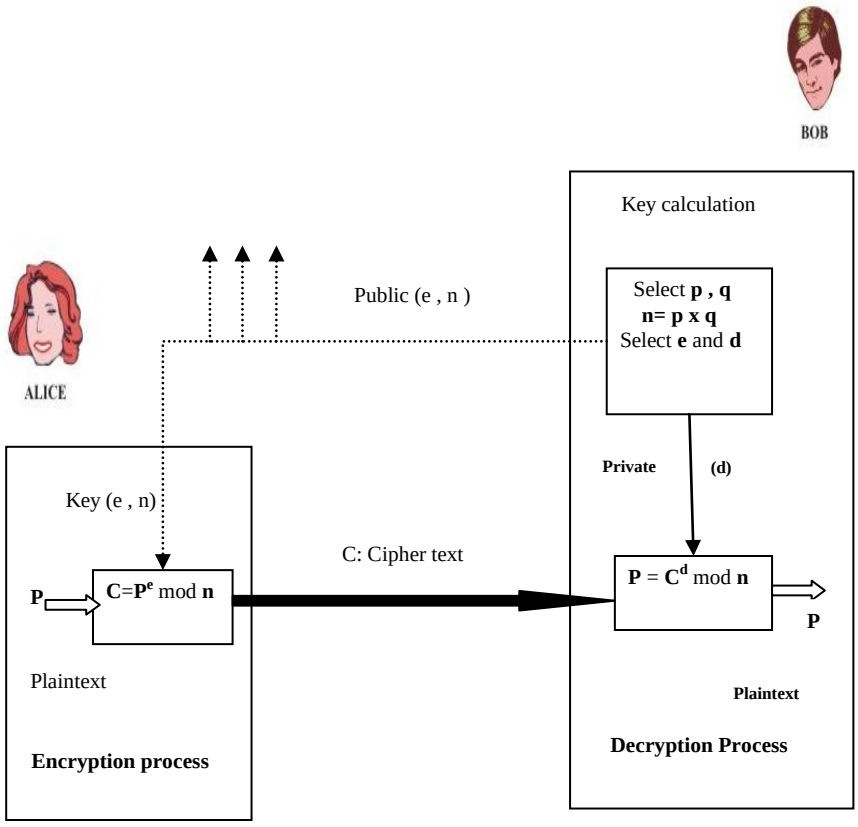

Figure 3: RSA Cryptosystem

STEP-2 PATH COMPUTATION

Source will start finding out shortest paths to destination. In case of route failure the immediate node will select the other shortest path to destination.

STEP-3 TEXT ENCRYPTION USING MODIFIED RSA CRYPTOSYSTEM

- Compute n = pq. n is used as the modulus for both the public and private keys.
- Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient function.
- Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co-prime.
- Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

STEP-4 CONNECTION TERMINATION:
After finishing communication, nodes will terminate the temporary network.

6. RESULTS

RSA security protocol stands for the Rivest, Shamir and Adleman who are the creator of the RSA. RSA is an asymmetric-key security protocol as it uses two different keys for its encryption and decryption purpose. It is the most popular and proven asymmetric key cryptography algorithm. It generates two key private key and public key. Private key is secrete to the user and public key is known to other who wants to communicate with the user. For this reason it is also known as public-key cryptography. It is the very first algorithm known to be suitable for signing as well as encryption, and was one of the first advances in public key cryptography

CPU and Memory Utilization
An algorithm should utilize minimum CPU resources as well as minimum memory (RAM). Figure below shows the process ID, Percentage of CPU and Memory used.

```
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      1018  7.9  2.1 119520 44436 tty7     Rs+  06:23   1:04 /usr/bin/X -cor
1000      1779  0.9  1.1 127704 22948 ?        S1   06:31   0:03 /usr/lib/vmware
1000      1871  0.5  1.0 181736 22076 ?        S1   06:31   0:01 /usr/bin/python
1000      1743  0.7  0.9 119636 20144 ?        S1   06:31   0:02 Thunar --sm-cli
1000      1746  0.9  0.7 116884 14584 ?        S1   06:31   0:03 xfdesktop --dis
1000      1785  0.1  0.6 149876 13784 ?        S1   06:31   0:00 nm-applet
1000      1744  0.4  0.6 106416 13504 ?        S1   06:31   0:01 xfce4-panel --d
1000      2782  0.6  0.6 113868 13184 ?        S1   06:35   0:00 /usr/bin/xfce4-
1000      1797  0.3  0.5  37948 11656 ?        S1   06:31   0:01 /usr/bin/python
1000      1752  0.1  0.5 112308 11448 ?        S1   06:31   0:00 /usr/lib/i386-l
1000      1741  0.7  0.5  25396 10572 ?        S    06:31   0:02 xfwm4 --replace
1000      2851  2.2  0.4  24984  9888 pts/1    S1   06:36   0:00 nam -r 5m AODV.
```

Figure 4: Percentage of CPU and Memory Utilized by RSA Algorithm

Figure below shows the percentage of CPU and Memory resources utilized by RSA Digital Signature. It is evident that RSA Cryptosystem is consuming fewer resources as compared to RSA Digital Signature.

```
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      1018 13.5  2.6 132608 55316 tty7     Ss+  06:23   7:47 /usr/bin/X -cor
1000      1779  0.5  1.1 127704 22948 ?        S1   06:31   0:17 /usr/lib/vmware
1000      1871  0.0  1.0 181736 22076 ?        S1   06:31   0:01 /usr/bin/python
1000      1743  0.3  1.0 144528 21264 ?        S1   06:31   0:11 Thunar --sm-cli
1000      1744  0.4  0.7 107472 15672 ?        S1   06:31   0:14 xfce4-panel --d
1000      1746  0.1  0.7 119220 15584 ?        S1   06:31   0:05 xfdesktop --dis
1000      1741  0.9  0.7 100276 14548 ?        S1   06:31   0:28 xfwm4 --replace
1000      1785  0.0  0.6 149876 13784 ?        S1   06:31   0:00 nm-applet
1000      3973  1.0  0.6 113836 13080 ?        S1   07:20   0:00 /usr/bin/xfce4-
1000      1797  0.0  0.5  37948 11656 ?        S1   06:31   0:01 /usr/bin/python
1000      1752  0.0  0.5 112308 11448 ?        S1   06:31   0:00 /usr/lib/i386-l
1000      4032  3.2  0.4  25016  9884 pts/1    S1   07:21   0:00 nam -r 5m AODV.
```

Figure 5: Percentage of CPU and Memory utilized by RSA Digital Signature

Energy Consumption

The Energy Consumed by RSA Cryptosystem is less as compared to RSA Digital Signature. The Difference has been showed in the following snapshots.

```
node 0 40.7822
node 1 40.6776
node 2 40.7212
node 3 41.4613
node 4 40.5426
node 5 41.7877
node 6 40.6284
node 7 40.5417
node 8 40.5425
node 9 40.7824
node 10 40.7767
node 11 41.1364
node 12 40.5428
node 13 40.6144
node 14 40.5427
+============+
Average Energy =  40.872
+============+
Total Energy of Nodes =   613.081
```

Figure 6: Energy of Nodes in RSA Digital Signature

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

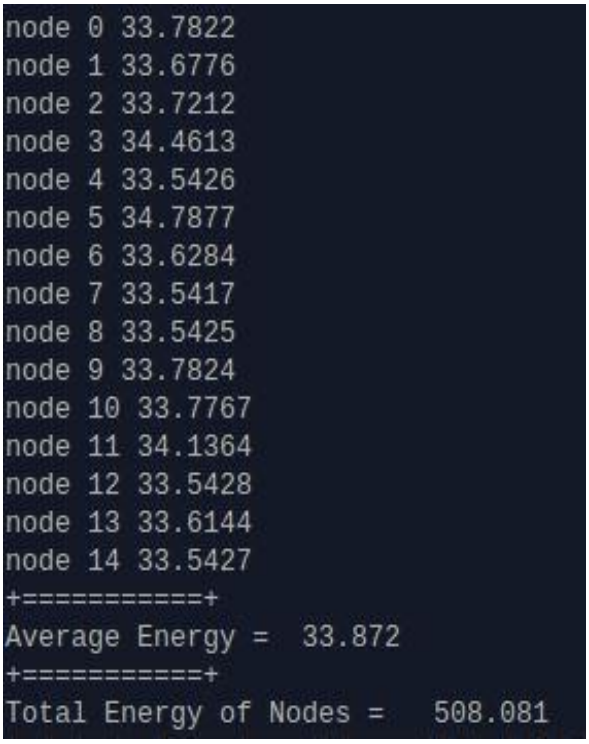

Figure 7: Energy of Nodes in RSA Cryptosystem

7. CONCLUSION AND FUTURE SCOPE

We have successfully Implemented RSA Digital Signature in Mobile ad-hoc Network. In future work we will reduce the complexity of the algorithm and save the energy of Mobile Nodes So that ad-hoc Network can utilize the energy of Nodes in efficient way.

REFERENCES

[1] **Vivek Saini , Ashok Kumar Saini (2013) "Performance Comparison of Routing Protocol (Proactive & Reactive) of MANET" International Journal of New Innovations in Engineering and Technology (IJNIET) Vol. 1 Issue 4 April 2013 38 ISSN: 2319-6319 .**

[2] **Fu Yongsheng, Wang Xinyu, Li Shanping (2008) "Performance comparison and analysis of routing strategies in Mobile ad hoc networks" International Conference on Computer Science and Software Engineering 978-0-7695-3336-0/08 $25.00 © 2008 IEEE DOI 10.1109/CSSE.2008.799.**

[3] **Kailash Pareek, Prof. K.P. Yadav (2013) "A New Algorithm For Secure Routing Protocols For Moble Adhoc Networks" International Journal of Latest Research In Engineering and Computing (IJLREC) ISSN:2347-6540 Volume 1, Issue 2 : Page No26-33, November-December 2013 .**

[4] **Pandit Savyasaachi J (2012) "A Survey on Energy Consumption in Routing Protocols for MANET Using Cross Layer" International Journal of Advanced Computer Research 2249-7277 ISSN (online): 2277-7970) Volume-2 Number-4 Issue-6 December-2012.**

[5] **Priya Shrivastava, Sushil Kumar Manish, Shrivastava (2014) "Study of Mobile Ad hoc Networks", International Journal of Computer Applications (0975 – 8887) Volume 86 – No 3, January 2014.**

[6] **Krishnan, M.B. Mukesh. Dr. Abdul Khader, P. Sheik (2011) "Authenticating and Securing End-to-End Communications through Encrypted Key Model for Mobile Ad Hoc Network" International Journal of Computer Applications (0975 – 8887) Volume 35– No.7, December 2011**

[7] **7 S. Basagni, M. Conti, S. Giordono and I. Stojmenovic: Mobile Ad Hoc Networks, IEEE Press Wiley, New York, 2003.**

[8] **Ajay Kushwaha, Hariram Sharma (2012) "Enhancing Selective Encryption Algorithm for Secured MANET" 2166-8531/12 $26.00 © 2012 IEEE DOI 10.1109/CIMSim.2012.16**

[9] **Ariel Stulman, Jonathan Lahav and Avraham Shmueli (2012) "MANET Secure Key Exchange using Spraying Diffie-Hellman Algorithm" 978-1-908320-08/7/$25.00©2012 IEEE**