IMPROVING PERFORMANCE AND SECURING DATA IN MANET WITH AES

Amol Bhosle[1]
Department of Computer Engineering, VIIT, Pune
amolabhosle@gmail.com

ABSTRACT:
Mobile ad-hoc network is wireless network composed of different nodes communicate with each other without having to establish infrastructure. The security of such network is a major concern. To improve the security of such network and to improve the efficiency of Adhoc on demand distance vector routing protocol technique proposed here is SMDNA (Securing MANET Data using Node Authentication) that combines the features of Symmetric and asymmetric cryptographic algorithms and digital signature. This protocol design provides the integrity, confidentiality, non repudiation and authentication with the help of AES, and digital signature. It shows better results in terms of end to end delay and throughput on varying number of nodes. This method also applied on other algorithms IDEA,DES. The results shows better performance with AES algorithm.

Keywords: Mobile ad-hoc, symmetric cryptographic, asymmetric cryptographic, confidentiality, AODV, digital signature.

1. INTRODUCTION

Ad-hoc networks are characterized by dynamic topology, self-configuration, self-organization, restricted power, temporary network and lack of infrastructure. Characteristics of these networks lead to using them in disaster recovery operation, smart buildings and military battlefields. Routing protocol in ad-hoc networks are classified into three main categories, proactive , reactive and hybride. In proactive routing protocols, routing information of nodes is exchanged, periodically. In reactive routing protocol routing information of nodes gathered on time when needed. In hybride the combination of the two are used.

A mobile ad hoc network has following features:
The cryptographic algorithms are classified into two different types such as symmetric and asymmetric.
In symmetric encryption method both sender and receiver share the common key value for encryption and decryption. It requires that the sender find some secure way to deliver the encryption/decryption key to the receiver. The effective key distribution needs to deliver key to the receiver. Large number of protocols provides various techniques. These protocols are to provide more secure but less performance. The public key cryptography or asymmetric cryptographic method solves the problems of key distribution. In this method, uses a pair of keys for encryption. The public key encrypts the data and corresponding private key for decryption. Each user has one pair of keys. The private key kept secret and public key knows by others. Any one wants to send some information to you they read your public key and encrypts the information. After you receive, the encrypted data using your private key to decrypt it. One issue with public key cryptosystems is that users must be constantly vigilant to ensure that they are encrypting to the correct person’s key. In a public key environment you are assured that the public keys to which you are encrypting data is in fact the public key of the intended receiver. The identification of correct public key of proper person is more difficult without using any third party.
In mobile ad hoc network, each mobile node acts as a host as well as a router.Ad Hoc on Demand Distance Vector routing protocol is a reactive routing protocol which establish a route when a node requires sending data packets. It has the ability of unicast & multicast routing. It uses a destination sequence number (DestSeqNum) which makes it different from other on demand routing protocols. It maintains routing tables, one entry per destination and an entry is discarded if it is not used recently. It establishes route by using RREQ and RREP cycle. If any link failure occurs, it sends report and another RREQ is made.But in existing AODV, there is no reliable security provided for the transmission of the data.

2. LITERATURE SURVEY

Shiva et al proposed [2] proposed the method that the digital signature based secure data transmission in wireless sensor networks. They used the asymmetric key crypto system (public) for the security. To generate the digital signature MD-5 hash function is used. Also RSA algorithm is used which provides digital signature as well as secrecy. The results are compared with AOMDV which is a extension of AODV protocol.

Changhui et al [1] proposed method that provide a scheme that with hash based message authentication code to overcome the shortcomings. Hash based message authentication code using cryptographic hash function such as SHA-1 in combination with secret key. It provides the integrity of information transmitted over a unreliable medium based on secret key. In this method HMAC checking and symmetric encryption used to replace complicated ECC to achieve secure communication.

M.A.Matin et al [6] proposed a method on symmetric encryption technique with AES algorithm in MANET and WLAN. Symmetric encryption is faster and requires less computational processing time. The increase in key size as well as block size,the security gets enhanced and linear cryptanalysis and differential cryptanalysis require more time to break the proposed cipher here.

Hongbo Zhou et al [4] proposed a method of autoconfiguration which is a method to achieve uniqueness of address allocation with the help of IP address for each node. In this authors used the method of SA-PKD which includes broadcasting of DAD (Duplicate address Detection) message. In DAD message it contains the Hash value of IP address of node and IP address signed with its private key.If a node receives a DAD message it calculates hash value of its own IP address. If it is same them generates NACK message and sends back to node N.

S.Thadvai et al. [3] proposed a method based on message recovery which includes message and the signature hence the communication cost is lower for the message recovery method. In this method they used the Authentication Encryption Scheme (AES) for message recovery

Mare.S.F. et al. [7] proposed a method that uses AES, RSA for securing sensitive data that assures integrity, authenticity and security.

Luis et al.[8] proposed the method a pair-wise key based scheme for forming secured private clusters in mobile adhoc networks. The solution tackles the problem of node authentication combined with traffic encryption in relatively small adhoc networks using proactive neighbour discovery and authentication.

Jerome Burke[5] discussed the various symmetric cipher algorithms and their key sizes, number of rounds required also size of block of data used. It shows the IDEA, DES3, Blowfish,RC-4 works on 64 bit block of data only. In terms of number of rounds Rijndael takes only 10 rounds.

Uttam Ghosh et al [9] proposed a ID based distributed dynamic IP configuration scheme for address allocation. They discussed the three categories namely best effort allocation; Leader based allocation and Decentralized allocation. And gave solution to overcome the problems arised by these three categories. For address detection they denied the concept of DAD scheme.

3. AODV PROTOCOL

It is an on demand routing protocol. At first all the nodes send hello message on its interface and receive hello message from its neighbors. This process is repeated periodically to determine neighbor connectivity and to update routing table entry. When a route is needed to some destination, the protocols start route discovery .It uses two term route request & route reply.

A] Control Messages in AODV:

• Route Request Message RREQ:

Source node that needs to communicate with another node in the network transmits RREQ message. AODV sends RREQ message. 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.

B] Route Discovery in AODV:

When a node "S" wants to initiate transmission with another node "D", it will generate a route request message (RREQ). This control message is forward to the neighbors, and those node forward the control message to their neighbors' nodes. This process continues until it finds a node that has a fresh enough route to the destination or destination node is located. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node. When RREP reaches the source node, a route is established between the source node "S" and destination node "D". Once the route is establish node "S" and "D" can communicate with each other. The following figure shows exchange of control messages between source node and destination node.

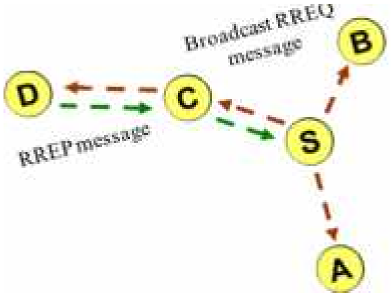


Figure 1: Route Discovery in AODV

When there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbors nodes, the RERR message is sent to the source node. When RREQ message is broadcasted for locating destination node i.e. from node "S" to the neighbors nodes, at node "D" the link is broken between "S" and "D", so a route error RERR message is generated at node "D" and transmitted to the source node informing the source node a route error.

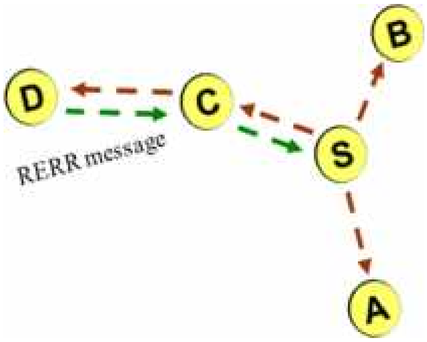


Figure 2: Route Error Message in AODV

Security Problem with Existing Ad hoc Routing Protocols

The main assumption of the ad hoc routing protocols is that all participating nodes do so in good faith and without maliciously disrupting the operation of the protocol. 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 [2].

Security Goals

In providing a secure networking environment some or all of the following service may be required.

1. Authentication: This service verifies the identity of node or a user, and to be able to prevent impersonation. In wired networks and infrastructure-based wireless networks, it is possible to implement a central authority at a point such as a router, base station, or access point. But there is no central authority in MANET, and it is much more difficult to authenticate an entity. Authentication can be providing using encryption along with cryptographic hash function, digital signature and certificates.

2. Confidentially: Keep the information sent unreadable to unauthorized users or nodes. MANET uses an open medium, so usually all nodes within the direct transmission range can obtain the data. One way to keep information confidential is to encrypt the data.

3. Integrity: Ensure that the data has been not altered during transmission. The integrity service can be provided using cryptography hash function along with some form of encryption. When dealing with network security the integrity service is often provided implicitly by the authentication service.

4. Availability: Ensure that the intended network security services listed above are available to the intended parties when required. The availability is typically endure by redundancy, physical protection and other non-cryptographic means, e.g. use of robust protocol.

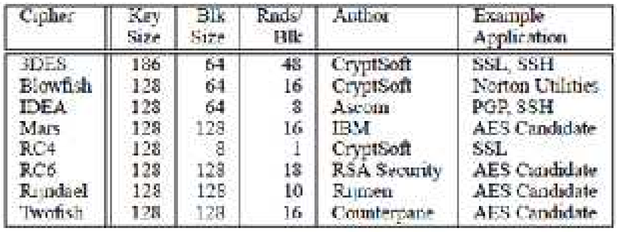
5. Non-repudiation: Ensure that parties can prove the transmission or reception of information by another party, i.e. a party cannot falsely deny having received or sent certain data. By producing a signature for the message, the entity cannot later deny the message. In public key cryptography, a node A signs the message using its private key. All other nodes can verify the signed message by using A's public key, and A cannot deny that its signature is attached to the message.

6. Access Control: To prevent unauthorized use of network services and system resources. Obviously, access control is tied to authentication attributes. In general, access control is the most commonly thought of service in both network communications and individual computer systems.

4. SYMMETRIC ENCRYPTION ALGORITHM

Table1 shows various private key encryption algorithms with their key size and blocks of data on which they are applied, Also the number of rounds taken by each algorithm to perform operation. Study shows that 3 DES and IDEA works on the 64 bit block of data. And rest of the algorithms work on 128 bits of data. Also in terms of number of rounds required. As compared to other symmetric algorithms AES is much more faster and store data in compressed format.[5]

Table 1. Comparision of Symmetric encryption algorithms



Cipher	Key Size	Blk Size	Rnds/ Blk	Author	Example Application
3DES	186	64	48	CryptSoft	SSL, SSH
Blowfish	128	64	16	CryptSoft	Norton Utilities
IDEA	128	64	8	Ascom	PGP, SSH
Mars	128	128	16	IBM	AES Candidate
RC4	128	8	1	CryptSoft	SSL
RC6	128	128	18	RSA Security	AES Candidate
Rijndael	128	128	10	Rijmen	AES Candidate
Twofish	128	128	16	Counterpane	AES Candidate

5. METHODOLOGY

As symmetric cipher algorithm allows us to store the data in a compressed encryption form which results in a small size database. Also it performs faster encryption/decryption. Due to these advantages here using symmetric cipher algorithm to perform data encryption and decryption. This will also serve confidentiality. Moreover combine the MD-5 and RSA public key algorithm to generate the digital signature.

The main advantage of using digital signature is it provides user authentication and data integrity and non-repudiation. As digital signature is akin to signing the document physically, it is the acknowledgement of the message so sender can not deny the message. [9]

This method works on the concept of node authentication for trusted nodes. Any node in the network is capable of assigning

IP address to other new node willing to join the network[2].If any malicious node willing to communicate in network then the access is restricted to that node. The method is tested on various symmetric cipher algorithms as IDEA, and DES. It shows better performance with AES.

VI. RESULTS AND DISCUSSION

The SMDNA model is implemented using network simulator 2.32. The simulation parameters are 1200 ×1200 sq.m area. 20 to 80 number of nodes. This SMDNA model is compared with the normal AODV model from different performance metrices such as to end delay,throughput.

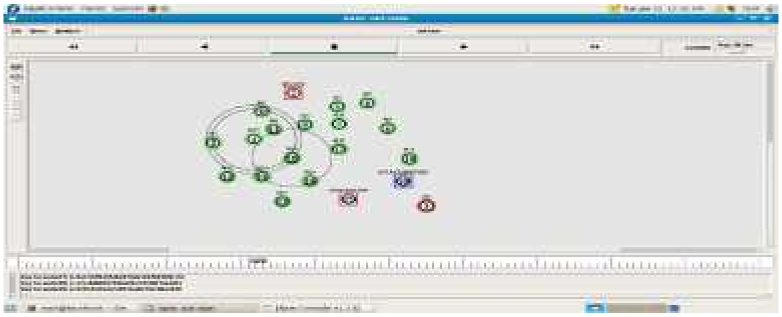


Figure 3: Simulation of nodes communicating

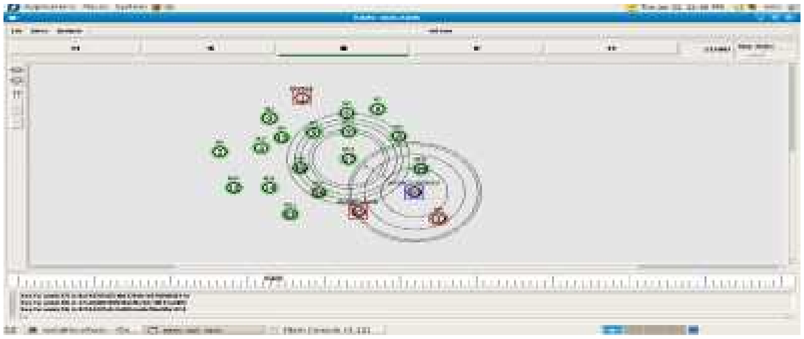


Figure 4: Attacking node

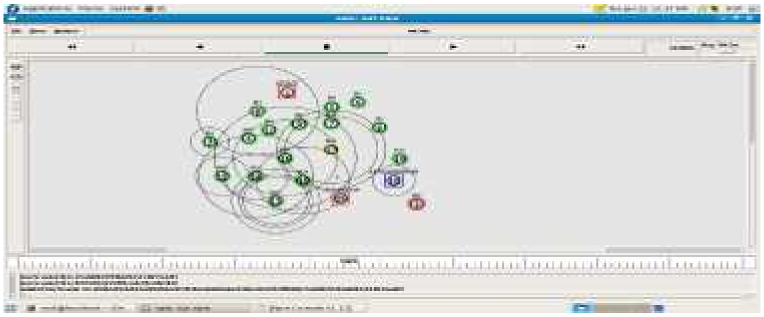


Figure 5: Change of route

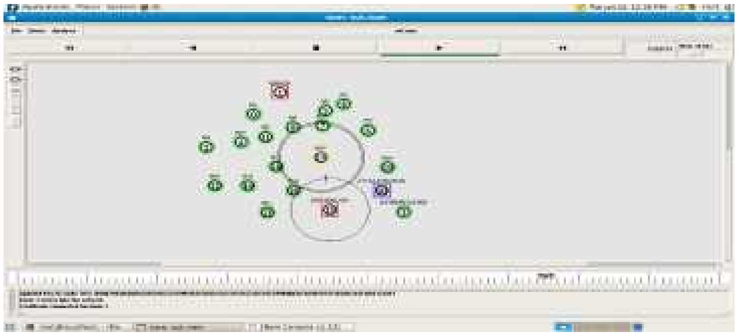


Figure 6: New node authentication

The simulation is done on Network simulator 2. The screenshots are as shown in figures. Fig 3 shows the number of nodes and start of communication which consists of 20 nodes. Fig 4 shows the attacking node that is node number 10 generates false information about route and tries to be act as authenticated node of the network. While the intermediate node checks for the digital signature it identifies that node number 10 is the attacking node, so the node is blocked and the route is made through the other node as shown in the figure 5.
Figure 6 also shows the new node i.e node number 3 tries to attach with the network. And after authentication steps the node 3 is declared as the authenticated node.

Following table shows the simulation parameters.

Table2. Simulation Parameters

Sr.No.	Parameters	Values
1	Simulator	ns-2.32
2	Simulation area	1200 ×1200
3	Propogation	Two Ray ground
4	Communication Traffic	TCP
5	Simulation time	10 sec
6	No.of nodes	20,40,60,80
7	Malicious node	1

A. End to End Delay

The End to End delay includes all possible delays due to buffering during route latency, queuing at the interface queue,retransmission delays at the MAC, and propogation and transfer times of data packets. Figure 7 shows end to end delay incurred in the normal AODV and SMDNA models. The end to end delay is reduced in SMDNA model as compared to the normal AODV model.
IT refers to the time taken for a packet to be transmitted across a network from source to destination

End to end delay D =Td-Ts

where Td is the packet receive at the destination
Ts –Packet send by the source node

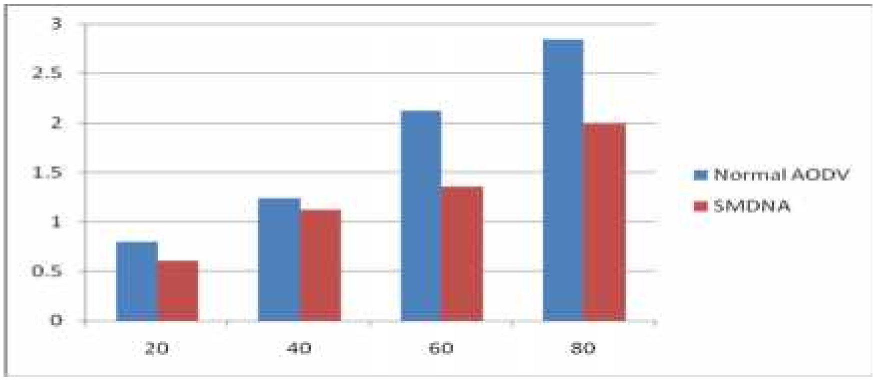


Figure 7. End to End delay Vs Number of Nodes

B. Throughput

Throughput is the amount of data receiver actually receives from the sender divided by time taken by receiver to obtain the last packet. Figure 8.shows the number of packets receiver received against the time. It shows the improvement in the throughput as the number of nodes increases.

It is one of the dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation i.e., information whether or not data packets correctly delivered to the destinations

Throughput = number of packets delivered / Time interval length

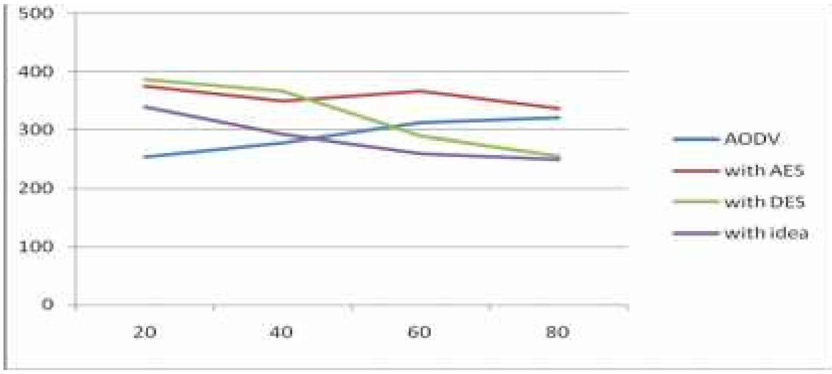


Figure 8. Throughput vs Number. of Nodes

6. CONCLUSION

The work proposed here is Securing data in mobile ad hoc network using the digital signature scheme applied on AODV routing protocol with AES. The result shows improved performance of AODV routing protocol with proposed method. In terms of throughput the percentage increase in throughput is 47.71% for 20 nodes , for 40 nodes it is 25.89% increase, for 60 and 80 nodes it is 17.28 % and 4.58% increase respectively.

In case of end to end delay the percentage decrease for 20 nodes is 25.44% , while in case of 40 nodes it is 9.13% decrease , in case of 60 and 80 nodes the percentage decrease is 27.30% and 30.32 % respectively.

This method works better with AES than IDEA and DES symmetric cipher algorithms.

REFERENCES

[1] Changhui Hu,Tat Wing Chim,S.M. Yiu,Lucas C.K. Hui, Victor O.K.Li “Efficient HMAC-based secure communication for VANETs” Computer Networks 56, Elsevier 2012.

[2] Shiva Murthy G.Robert John D’Souza, Golla Varaprasad “Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks” IEEE sensors Journal vol.12.No.10, October2012.

[3] S.Thadvai, D.N.Tiwari, D.Jena, M.Ma ”A novel authenticated encryption scheme with convertibility” Mathematical And Computer Modelling, Elsevier(2012)

[4] Hongbo Zhou,Matt Mutak,Lionel Ni “Secure autoconfiguration and Public key Distribution for Mobile Ad-hoc Networks” IEEE 2009

[5] Jerome Burke, John macdonald, Todd Austin “Architectural support for fast Symmetric key Cryptography”

[6] M.A.Matin,Md.Mohir Hossain et al ”Performance Evaluation of Symmetric Encryption Algorithm in MANET and WLAN” IEEE Technical postgraduates 2009 International conferernce.

[7] Mare,S.F. “Secret data communication system using steganography, AES and RSA” SIITME IEEE (2011)

[8] Luis Sanchez, Jorge Lanza,Luis Munoz,Kimmo Ahola,alution “Securing the communication in Private Heterogeneous Mobile Adhoc Networks”,Springer (2008)

[9] Uttam Ghosh, Raja Datta “A secure dynamic IP Configuration scheme for mobile ad hoc networks” Ad hoc Networks 9(2011) 19-28. Elsevier(2011)

[10] William Stallings “Cryptography and Network Security” Fourth Edition, Pearson Education Asia (2006)

[11] www.isi.edu/nsnam/ns

[12] ns2 tutorial, Multimedia Networking group, Jiamping Wang.