HASHED SYMMETRIC KEY ENCRYPTION BASED VBSR

[1] R.RAJAMOHAMED, [2] Dr. V. RAJAMANI

[1] Research Scholar Department of Electronics and Communication Engg, St.Peter's University Chennai, India
[2] Principal Veltech Multitech Dr.Rangarajan Dr.Sagunthala Engg.college ,Avadi,Chennai,India -600062
E-mail: [1]rrmd_77@yahoo.com , [2]rajavmani@gmail.com

ABSTRACT

Security impact on mobile ad hoc network increases more since there is no architecture and high mobility of nodes along the environment. Security features include providing authentication and confidentiality. Both these services insist that the messages should be encrypted and decrypted using some keys either public key and private key. Before encrypting the information to be secure, the users in the network should authenticate themselves since there is a central point to control the users. In this paper, we have taken our VBSR protocol for the implementation of authentication mechanism. In this work, a hash value is found then it is checked at receiver for authentication that the message is generated by the authorized sender and a secure protocol is developed called Hashed VBSR (HVBSR). The hash value 'H' is found using the hash function since the hash function can be taken as a way to compute the Message Authentication Code (MAC). Since the high dense of mobile nodes cannot be provide best security, the mobile nodes must be formed as groups. In order to provide security, there are pre-requirements like public key infrastructure (PKI), group key management and key agreement and key agreement so on. Then these keys are used in the encryption/decryption algorithms such as symmetric key algorithms and asymmetric key algorithms.

Keywords: *MANET, Security, Hash function, MAC, VBSR.*

1. INTRODUCTION

Wireless networks are growing rapidly in the last few years. In wireless networks, there are two classifications: Infrastructure based wireless networks and Infrastructure less or ad-hoc wireless networks. Most wireless networks deployed at present are IEEE 802.11 Wireless LANs. So there are pre established wired infrastructure for wireless LANs to connect various access points. But there are no wired connections in wireless ad hoc networks. Since the nodes are mobile nodes and there are no such pre-existing infrastructure. Nodes with wireless capability form an ad-hoc network in real time. In ad hoc network, the mobile nodes are working as a normal mobile node and as well as central coordinators which are forwarding the packets from one mobile node to another mobile node. Ad-hoc network is ideal for battlefield or rescuer areas where fixed infrastructure is very hard to deploy. Wireless ad hoc networks, as a new wireless paradigm of wireless communication, have attracted a lot of attentions recently. An ad hoc network is considered as a collection of wireless mobile nodes that are capable of communicating with each other without the use of any centralized administration. It is formed on-the-fly, and employs multi-hop routing to transmit information. The primary advantage of such a network is the underlying self -organizing and infrastructure-less property, which provides an extremely flexible method for establishing communications in situations where geographical or terrestrial constraints demand totally distributed networks, such as battlefields, emergency, and disaster areas. While the great flexibility of wireless ad hoc networks also brings a lot of research challenges, one of the important issues is security. Recent researches have shown that wireless ad hoc networks are highly vulnerable to various security threats due to their inherent characteristics. As ad hoc networking somewhat varies from the traditional approaches, the security aspects that are valid in the networks of the past are not fully applicable in ad hoc networks. A mobile ad-hoc network is a collection of autonomous nodes that communicate with each other. Ad-hoc network needs security mechanisms for secured communication. Providing security for ad-hoc mobile nodes is a very difficult task because all the mobile nodes are without any infrastructure. Since there is high mobility [1] among mobile nodes cannot be implemented any security mechanism without a central nodes has been capability to store the key pairs [2] [3] of all mobile nodes. Suppose the central node is moving frequently, then all key pairs of mobile nodes will be destroyed. Mobile nodes form an ad-hoc group for secure communication. In traditional wireless networks, a key distributed system is available as a third party that acts as a intermediate node between nodes of the network. Ad-hoc networks do not have a trusted third party. In group key agreement [4] [5], multiple nodes form a group and generate a common secret key to be used to exchange information securely. A group member can leave or a new group member can join in the existing group. At that time, the group key agreement protocol needs to address the security issues related to the membership changes due to node mobility. In group key agreement protocol, all nodes within the group selects a group key for secure transmission. The value of membership change requires frequent change of group key. So with this algorithm has been formed the secure algorithm with grouping the members as well as encryption.

Low resource availability necessitates efficient resource utilization and prevents the use of complex authentication and encryption algorithms. Most often, mobile nodes in ad hoc networks rely on batteries as their power source, and may also have constrained computational abilities. Traditional PKI-based authentication and encryption mechanisms are relatively expensive in terms of generating and verifying digital signatures, which limit their practical application to wireless ad hoc networks. Symmetric cryptography is more efficient due to its less computational complexity, in which the communicating parties share a secret key[6] [7]. But the foremost problem when using it in wireless ad hoc networks. It is thus challenging to develop or define some new efficient cryptographic algorithms for designing an efficient key management scheme.

2. RELATED WORK

In [8], T. Peer Meera Labbai and V. Rajamani have discussed the secure VBOR that includes the computation of MAC value. They have found the MAC using the function ‘C’. It consists of the shared key between the users ‘i’ and ‘j’. MAC is found in the process of route discovery. RREQ messages are encrypted using shared secret key $S_{i,j}$. It has no indirect encryption like hash functions. So the attackers can easily find the MAC value by substituting any of the possible keys. Also Secure VBOR includes every intermediate nodes address along with the encrypted RREQ messages. It increases the memory capacity.

Bivariate polynomials have already been used in other works to dynamically allow new nodes joining the network without the need of any external trusted party, inspired on the original work of [9]. Some works [10,11] constructed decentralized flexible dynamic group key distribution schemes by means of using polynomials in two variables. The goal is to generate common group secret keys. Saxena et al. [11] used this technique to establish pair wise keys in a non-interactive way in a mobile ad-hoc scenario.

Other works that consider distributed cryptography over MANETs are the threshold signature scheme [12]. They also make use of secret sharing techniques, although their approach is different to ours. In the case of [12] the shared secret changes according to the set of nodes that cooperate to produce a signature.

3. PROPOSED SCHEME

3.1 Problem Statement

Let m be the number of users (1,…..m). Each user is assigned by a pair wise key (public key and private key) such as P_u, P_r. In most of the previous works, a shared secret key is generated. No other cluster formation was there. Since there is no infrastructure in mobile ad hoc networks, the members have to interact among themselves without the use of any central coordinator. In our scheme, all the members are enrolling themselves in the cluster which is headed by a cluster head.

3.2 Formation of Cluster Head

Among m users, one member is selected as a cluster head. The cluster heads are elected as per the following algorithm,

Step 1: Assume there are m users (1,….m)

Step 2: Calculate the distance between one user and another user

Step 3: Step2 is repeated until distance is calculated for all the nodes with other nodes. Form a Virtual Wireless Mesh Networks.

Step 4: One node is selected as a cluster head based on the node's distance with all other nodes with condition that $D_{CH, (i,\ldots m)}$ is equal to 1.

Step 5: Cluster Head (CH)= I such that I has equal distance with other(n-1)nodes(j,….m) that is $D_{i,j} = D_{(i, (k,\ldots m))} = 1$

Step 6: When there is high mobility, the cluster head may be changed from I to any of the (n-1) nodes based on step 5.

4. MODULES

In our approach, there are two modules namely,

a) Secure one time key management
b) Hashed VBSR

According to cryptographic algorithms, there are no such algorithms as secure. The proposed approach gives a better security to key management as well as to data transmission. Since there is only one key which is generated by the cluster head, there is no possibility of losing the security.

4.1 Secure One-Time Key Management

The nodes of a network are formed as clusters. Each cluster is headed by a cluster head. Cluster head is selected as per section 3.2. The cluster heads are generating the one time keys to put it in the hash function. At a time, only one key is generated by the cluster head. That key is not usable at next time because there are many more attacks possible in mobile ad hoc networks. This one time key is passed among other nodes of the cluster so that nodes can deploy key management functions and can do many cryptographic functions. Cluster head creates a one-time key for every transaction. Thus the security of all transaction happened through cluster head. Cluster head transmits this one-time key to all the nodes inside the cluster by encrypting using it's private key. Every non cluster head nodes are decrypting the information using the cluster head's public key.

CH $\longrightarrow$ one time key K_{OT}

CH $\longrightarrow$ $E_{PR}^{CH}(K_{OT})$

Other nodes $\longrightarrow$ $D_{PU}^{CH}(K_{OT})$

4.1.1Route Discovery

The route discovery phase allows a source node S that wants to communicate securely and privately with node D to discover and establish a routing path through a number of intermediate wireless mobile nodes. At first time, there are no intermediate nodes those are knowing about the source node S and destination D. The source node S triggers the route discovery phase by sending a route request message to all nodes within the cluster.

In this approach, DSR protocol is taken as the base routing protocol. In DSR, the intermediate nodes play a main role since every intermediate node has route cache to deliver the route back to the source node if it has the route in its route cache. HVBSR safeguards the route discovery and makes use of some cryptographic tools. In HVBSR, only the end nodes have to be secured. It does not impose any cryptographic validation and verification of traffic at intermediate nodes for decentralized environment; finally, it reduces the routing and control traffic overhead and protects end nodes against attacks. In this secure route discovery, any malicious node between source S and destination D could not identify the original request because the message is encrypted with one-time key that is generated by cluster head.

$$M = E_{OT}\{RREQ\,.SA.DA\}.SA.DA \quad (1)$$

Upon receiving this message, each intermediate node decrypts the data by using the shared one-time key of that cluster. Also each node adds its information for example, its IP- address along with the message if it is not having any route to the particular destination D.

4.2 Hashed VBSR

The message 'M' of (1) is subjected to a hash function 'H'. Then hashed value is given as input to the encryption function E.

$$M \xrightarrow{H} H(M)$$

$$H(M) \xrightarrow{PR^{CH}} E_{PR}{}^{CH}(H(M))$$

$$E_{PR}{}^{CH}(H(M) \xrightarrow{PU^{CH}} E_{OT}(E_{PR}{}^{CH}(H(M))$$

Thus it provides both authentication (message is first encrypted using the private key of the cluster head) and confidentiality (encrypted message is again encrypted using the one-time key of the destination)

5. PERFORMANCE ANALYSIS

Simulation study has been carried out to show the performance of the proposed secure VBOR protocol. Simulation results have been compared for different number of nodes 30, 40 and 50 in terms of packet delivery ratio, energy consumption, overhead and delay.

Table 1: Simulation Parameters

Parameter	Value
Test Area	1500m x 1500m
Channel type	Wireless channel
Radio Propagation	Two Ray Ground
Antenna type	Omni antenna
Interface Queue type	Drop tail with priority queue
Interface Queue length	50
Transmission Range	250m
Number of Nodes	100
Transmission Bandwidth	1Mbps
MAC	IEEE 802.11
Mobility Model	Random Waypoint
Traffic type	VBR, UDP
Packet Size	512 bytes
Initial Energy	100 Joules

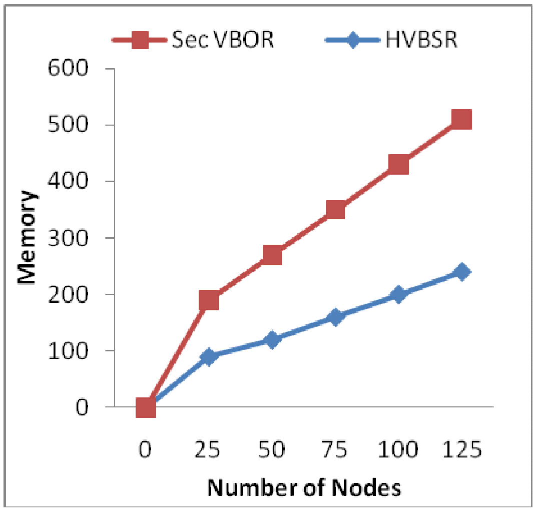

Figure 1: Memory with Number of Nodes

As per the memory to store the keys at member nodes as well as in gateway members, the ECC makes the process as easy as possible. Since the one-time key size(32 bits) is small in our HVBSR, the storage capacity at nodes are very smaller than the other symmetric key types like AES. In our key management protocol, the keys are created and shared by cluster head for that cluster only. But in Secure VBOR, each node has to maintain the keys of it with itself and it has to deliver its public key to group member (GM) to generate a shared secret key. Thus our approach consumes very lower memory storage cost than Secure VBOR approach.

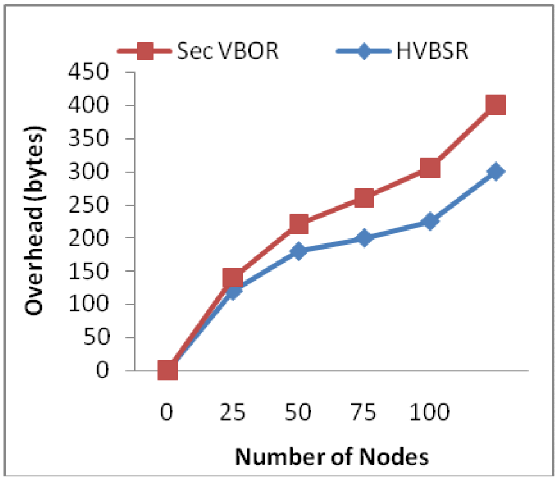

Figure 2: Routing Overhead with Number of Nodes

Figure 3 shows the variation in overhead with number of nodes in route discovery phase. Secure VBOR has high overhead when compared to HVBSR since there is no one-time key for transmission. Secure VBOR reproduces same public key and private key pairs of sender and receiver.

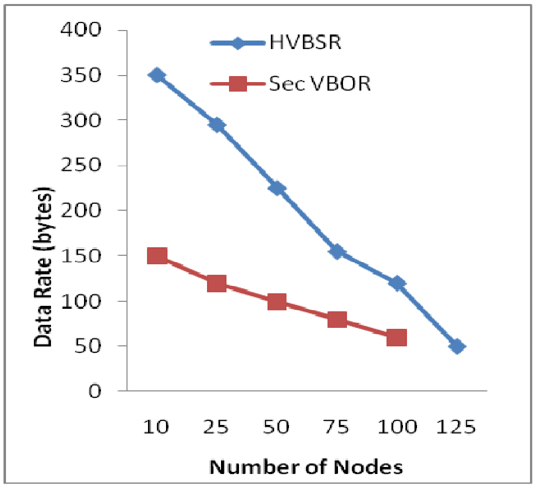

Figure 3: Variation of Packet Delivery Ratio with Number of Nodes

Variation of packet delivery ratio with number of nodes is shown in Figure 5. Packet delivery ratio can be calculated as the ratio between the number of data packets that are sent by the source and the number of data packets that are received by the destination. Packet delivery ratio decreases when the number of nodes increases to 50, 75, 100 nodes. 90% packet delivery ratio is decreased to 40% due to large number of nodes.

6. CONCLUSION

MANET needs more security because of the nature of mobile nodes. This work gives security to the Variable bit rate source routing protocol (VBSR). When compared with public key cryptography, symmetric key cryptography gives more security and less memory storage to the ad hoc networks because the nodes have to secure their keys with themselves. Here the malicious nodes could not get the data since the hash value is computed by cluster head and its members only. In this work, the nodes are authenticated and then the cluster members are decided then the cluster head is selected based on the distance among the other nodes. The data is transmitted with confidentiality that no malicious and selfish node can get the hashed and encrypted data.

REFERENCES:

[1] T. Peer Meera Labbai and V. Rajamani. “A Variable Bit-Rate On- Demand Routing Protocol for Mobile Ad Hoc Networks”, *International Journal of Ad hoc, Sensor and Ubiquitous computing*, Volume 3, 2012, 31-40.

[2] R.Rajamohamed and V. Rajamani, “A Modified Variable Bit Rate Source routing energy efficient Protocol for mobile ad hoc networks”. *International journal of IJEIT*, Volume12, 2012, pp -177-182.

[3]] Rafaeli S, Hutchison D. “A Survey of Key Management for Secure Group Communication”. *ACM Computing Surveys*, 2003, Vol. 35(3): 309–328.

[4] Minghui Zheng, Guohua Cui, Muxiang Yang, Jun Li. “Scalable group key management protocol based on key material transmitting tree”. *Proceeding of* ISPEC’07, LNCS 4464, and Springer-Verlag, Berlin. 2007, 301-313.

[5]] Mcgrew D A, and Sherman A T. “Key Establishment in Large Dynamic Groups Using One-Way Function Trees”. *Technical Report* No. 0755, TIS Labs at Network Associates, Inc., Glenwood, Md. 1998.

[6] Steine M, Tsudik G, and Waidner M. “Diffie-Hellman Key Distribution Extended to Group Communication”. *In SIGSAC Proceedings of the 3rd ACM Conference on computer and Communications Security*, ACM, New York, 1996, p. 31–37.

[7] Rodeh O, Birman K, and Dolev D. “Optimized Group Rekey for Group communication Systems”. *In Proceedings of ISOC Network and Distributed System Security*, 2000.

[8] T. Peer Meera Labbai and V. Rajamani. “Message Authentication Code based Secure Group key Management protocol for Mobile Ad Hoc Networks”, *International Journal of Ad hoc, Sensor and Ubiquitous computing*, Volume 3, 2012, 31-40.

[9] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung, *Perfectly-secure key distribution for dynamic conferences, in: Proceedings of Crypto*’92, LNCS, vol. 740, Springer-Verlag, 1993, pp. 471–486.

[10] J.Anzai, N. Matsuzaki, T. Matsumoto, A quick group key distribution scheme with entity revocation, in: *Proceedings of Asiacrypt*’99, LNCS, vol. 1716, Springer-Verlag, 1999, pp. 333–347.

[11] V. Daza, J. Herranz, G. Sa´ez, Constructing general dynamic group key distribution schemes with decentralized user join, in: *Proceedings of ACISP’03, LNCS*, vol. 2727, Springer- Verlag, 2003, pp. 464–475.

[12] N. Saxena, G. Tsudik, J.H. Yi, Efficient node admission for short-lived mobile ad hoc networks, in: *Proceedings of ICNP*’05, 2005, pp. 269–278.