Indian Journal of Science and Technology, Vol 9(26), DOI: 10.17485/ijst/2016/v9i26/95137, July 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Cluster Based Mutual authenticated key agreement based on Chaotic Maps for Mobile Ad Hoc Networks

Arshad Ahmad Khan Mohammad[1*], Ali Mirza[2] and Srikanth Vemuru[1]

[1]KL University, Guntur - 522502, Andhra Pradesh, India; ibnepathan@gmail.com, alimirza.md@gmail.com
[2]DMSSVH College, Machlipatnam - 521002, Andhra Pradesh, India; vsrikanth@kluniversity.in

Abstract

Implementing security in mobile ad hoc networks is very challenging due to its dynamic, heterogeneous and distributed nature. In order to deploy security most important pre requisite is '*authentication*'. However, providing security based on public key infrastructure with central third party authentication is difficult to deploy in MANETs Environment. Energy efficiency is another powerful factor due to its constrained battery power of nodes in MANETs. **Methods/Analysis:** In order to achieve security along with energy efficiency, we design & evaluate mechanism based on chaotic maps and knapsack algorithm, which addresses two vital characteristics: authentication & lifetime of network. We divide the MANETs into number of clusters with cluster heads and assign the key management task to cluster heads. **Findings:** Proposed work achieves the network life time based on new metric called 'Optimized data packets processing capacity' and authentication with the help of Chebyshev polynomials. **Application/Improvements:** Our proposed scheme abstains from computing overhead such as modular exponentiation and scalar multiplications of an elliptical curve. Moreover it is robust to different network attacks and assures that the secrete *session* key is established only between two intended entities.

Keywords: Authentication, Cluster, Chebyshev Polynomials, Key Agreement, MANETs, Optimization

1. Introduction

The importance of computing devices and their connectivity has become mandatory in our daily life. Earlier the connectivity of computers was made using wired network, which worked for a long time. Later, there was a high demand for wireless networks. It was achieved by wireless local area networks (WLAN) based on IEEE 802.11 standards. However next generation demands to develop wireless communication system with independent mobile users. Such networks are crucial in emergency services, risk operations, disaster recovery, military operations, conferencing, and electronic class rooms. This need can be met using Mobile Adhoc network (MANETs in short). In the first generation, wireless communication networks were based on analog technology. It primarily aimed to provide voice and data communication with low data rates, with AMPS (advanced mobile telephone system) technology. It supported 40khz spectrum with 832 channels and 10kbps data rate. After this, many innovations took place in wireless communications. Broadband features with mobility and multimedia transmission with QoS support were introduced. 2nd generation is based on digital multiple access technologies like (TDMA, CDMA), example of second generation systems are GSM, cordless telephone, DECT & PACS, in which GSM uses TDMA technique. Then the concept of GPRS, based on radio technology was introduced. This was called 2.5 generation or 2.5G, where packet switching technique was applied to GSM network. In it packets were broke into small chunks to have flexible data rates and continuous connectivity to network. This evolution is named as 3G. Later on, the concept of *infrastructure less network* was introduced by DARPA project. It is named as packet radio network (PRNET), where several wireless nodes communicate with one another on a battlefield using packet

*Author for correspondence

switching technique. It introduced a multi hop communication over wide-range extensions of ALOHA. ALOHA came with the concept of broadcasting property of radio signals to send/receive data packets in a single hop communication. The PRNET had a technical capability of self-organization and self-initiation. It means that, the nodes in a network organized themselves and finds the radio connectivity even in the absence of base station. PRNET was very much different from wired network due to its characteristics like absence of infrastructure, peer to peer networking and distributed nature. These qualities helped in the evolution of *Mobile ad hoc network* (MANETs).

The design goal of MANETs[1]is to support the network anywhere and anytime. MANETs are infrastructure less, self configured & self maintained. It is a wireless network with heterogeneous mobile devices (nodes), connected to form a dynamically varying network topology. It does not have any fixed infrastructure or a central coordinator or a base station to control the network communication. Every node possesses network intelligence to act as a router and also as a host. This means, the MANETs behave as a peer to peer network. The nodes are connected using more than one link, heterogeneous radio communication and can act in a standalone fashion. Due to these characteristics, the MANETs are suited well for a situation, where network infrastructure is incontinent to setup, and the network is cost and/or time effective.

Deployment of security in MANETs environment very much challenging[2,3] due to its peer to peer, dynamic, heterogeneous and distributed network nature; moreover there is no clear line of defense for designing security. Constrain battery power & computation capacities of nodes make MANETs vulnerable to develop security solutions. Hence MANETs require Security mechanism which must provide security as well as address the MANETs characteristics. In order to deploy security most important, simple and convenient pre requisite is 'mutual authenticated key agreement'. It is a process in which two communicating entities in a network authenticated each other and shares a secrete key among them as a function of information contributed by each other. Mutual authenticated key agreement is vital solution to protect the network environment from unauthorized entities and assures that the *secrete session* key is established only between two intended entities. It is applicable for MANETs as Nodes in a MANETs are autonomous so that they can prove and verify their authenticity without any external authority. As, authentication is well suited for internet based applications requiring higher levels of security[4,5].

Energy-Efficiency is another powerful considerable factor in MANETs, as communicating devices in a network are battery powered and it is not possible to recharge or replace the batteries during the risk or military operations, thus available energy of nodes limit its overall operation in network. Therefore, network lifetime effectively depends on the battery life of nodes. Battery drainage of node is due to data transmitting, receiving and processing of data packets and majorly to perform cryptographic operation, if any. So during the cryptographic operations minimizing energy consumption is most important issue to develop a security mechanism in MANETs. In MANETs environment Security protocol main goal is not only just provide the authentication, authorizing but also concentrate on network life time. Thus energy and security are most considerable characteristics to develop a security mechanism in MANETs. Moreover, design of mutual key agreement energy efficient protocol is very much essential in distributed environment in order to make network nodes to self competent in infrastructure less environment

Providing security along with energy efficiency is main requirement in resource constraint environment. For MANETs environment many security schemes[6] and energy efficiency schemes[7] are proposed, but unfortunately all these schemes are not well suited for MANETs application such as in battle field. Thus a single process is very much desirable, which combines both security and energy efficiency. In order to achieve the goal we present a method to provide security along with energy efficiency for MANETs called "Cluster based mutual key agreement scheme based on Chaotic Maps for MANETs". Proposed work achieves the energy efficiency is based on novel metric known as 'Optimized data packets processing capacity' and achieves the security with the help of Chebyshev polynomials. Although there was a lot of research work carried out by researchers to provide security based on different methods but our proposed scheme abstains from computing overhead such as modular exponentiation and scalar multiplication of an elliptical curve inorder to cope with dynamic heterogeneous environment of MANETs. Moreover it provides the method to achieve energy efficiency in network.

The rest of the discussion is organized as follows: 2nd section briefly introduce the security challenges of

MANETs. In section 3 discusses about proposed novel metric. Proposed security mechanism discussed in4thsection. Section 5 shows completely about the performance evaluation and results .Our work ends with conclusion & the future work.

2. Security In MANETs

Implementing security[8,]in MANETs is challenging task due to its characteristics like dynamic variation in network topology, constrained resource, imprecise state information, and absence of central coordination, hidden& expose node problem and wireless medium. Each node in a MANETs acts as a host as well as router that means it acts as a peer to peer network, which is a fundamental vulnerability and there is no perfect line of defence for designing security as well as no well defined place to deploy a security solution. Due to heterogeneous nodes and their physical capture, MANETs are vulnerable. Hackers may sneak into the network through these subverted nodes & perform intensive task like cryptographic computation due to constrained computational capacity.

Single hop communication in MANETs is possible through link layer protocols and multi hop communication is possible through network layer protocols. Both protocols assume that mobile nodes in a network are cooperative& coordinate in communication process; but in hostile environment this assumption is not valid. Cooperation is assumed, but not compulsory in MANETs. Malicious attackers can easily interrupt the operations of network, by not following the specifications of protocol. The functions of network layer are routing and forwarding of packets. But both are vulnerable to malicious activities, leading to various types of crashes in network layer.

In order to deploy security in any network environment most important prerequisite is 'authentication' and security strength of any communication network protocol depends on its key management technique. In literature number of secure protocol proposed based on key management in MANETs. These protocols mainly categorized into two types[9,10].

1. distributed key management protocols
2. centralized key management protocols

Distributed protocols[11-13] based on Group 'diffie-Hellman Key' procedure, in which two intended nodes generates a random number such a way that intruder has no chance of guessing it. These protocols suffer the overhead of multiple public key operations and not well suited for delay sensitive applications. Centralized key distribution protocols[14-16] based on 'Key pre distribution '(KPS) concept; these protocols relay on trusted third party, which shares the secrete information to other nodes in a network before group communication. Thus privileged users can compute certain keys and participate in communication. Centralized protocols suffer from single point of failure. Distributed key management protocols based on 'shared key' solution assumed that nodes in a network are good with proper behaviour. But this assumption is not true in MANETs environment. With the introduction of chaos theory in cryptography, many cryptographic algorithms have been developed, such as symmetric key encryption[17,18], asymmetric key encryption[19,20] and hashing[21,22].In order to improve security along with less overhead, chaos based key agreement protocols have been developed, such as two party key agreement protocols[23-26] and multi party key agreement protocols[27-30]. But none of these protocols considered the energy efficiency in their approach.

Our work main aim is to achieve secure communication with security goal authentication and efficient energy utilization to achieve network lifetime in order to cope with dynamic distributed network topology of mobile ad hoc networks. As authentication is the way to achieve integrity and non-repudiation in data communication. In order to achieve our aim we divide the network into number of groups based on existing work CGSR[31]. Each group contain Cluster Head (CH), Cluster Member (CM) and Gate Way (GW), Where CH is responsible for organization of cluster and inter cluster communication is the responsibility of GW. Our work is the extension of CGSR with security feature and energy efficient concept. Cluster head election is based on metric called optimized data packets processing capacity of node. It is calculated based on current traffic & residual energy of node.

Each node in a network agrees a public key pairs used for end to end security, and generate a secure session key with the help of Chebyshev polynomials[32]. Chebyshev polynomial's composition property introduces the concept of two entity key agreement concept that allows two communicating entities to exchange public keys through an unsecured medium and generate a shared secured key between them. Work[33-35] used Chebyshev polynomial's for authenticated key agreement but in their approach they assume that sharing of private information is through some secure channel but it is not possible in MANETs environment. These works motivate us to come with a new method to provide mutual authenticated key agree-

ment in MANETs. Our work contribution mainly is as follows:

Selection of Cluster head by "Optimized Data packets processing capacity" of nodes based on knapsack algorithm

Authentication based on Chebyshev polynomial's composition property.

3. Optimized Data Packets Processing Capacity of Node

In MANETs, due to its characteristics delay and energy are the parameters closely related to network life time, improving these characteristics could leads to improve the network life time. The prime focus is to enhance these characteristics by data traffic and makes the suitable environment for data traffic. As MANETs is a peer to peer network, nodes need to perform the function of routing. Thus every node in a network has buffer space (input and output buffer) to hold packets, whenever node act as a router packets stay in a node buffer before and after processing the packets. During communication if node becomes 'bottle neck node' such as the number of packets sent to node is greater than its capacity then it will drop the packets. In MANETs when packet arrives at input interface of an intermediate node (router) then it undergoes three steps before departing the packets.

1. Packet is put in input queue and forwarded until it reaches the end of the input queue and waits for checking
2. Processing module of node remove the packet from input queue and take the decision about the packet according to its module (Routing table to find its path)
3. Packet is put in output queue and forwarded until it reaches the end of the output queue and waits for its turn to send.

Packet loss occurs due to, packet arrives at input queue higher than its processing rate and packet departure rate from its output queue is less than its processing rate. To avoid the packet loss in MANETs due to bottle neck node we introduced the concept of "Optimized Data packet processing capacity of node" with the help of knapsack algorithm. In our previous work[36] we used Knapsack algorithm to calculate the optimized information processing capacity of a node with respect to current traffic & residual energy. However our work is used to calculate data processing capacity of node with respect to energy drain rate and delay, where we consider all the packets have same size expecting control messages. We maximize the data packets process from node as much as possible subject to minimize the energy drain rate and delay".

We considered MANETs with nodes 'Zi' with energy capacity of 'E' Joules; we are considering 'Pi' packets to be process through it. Packet sayP1has[x] k bits of data and takes 'Ed' energy drain rate and 'T' delay to process through node. We need to transmit as much as data from node 'Zi' within a available delay and energy drain rate, which in turn need to find the subset of data packets such that in below conditions

1. All processing data packets have combined with size(bytes) at most of 'Ed' joules/seconds
2. The total data packets process by node as much as possible
3. Node cannot process apart of packet(which should either hole/nothing)

We have derived the equation for the energy drain rate and data rate required by a node to process the data packets when it becomes an intermediate node in a multi-hop MANETs environment, where we need to calculate the optimization.Table 1 show the notation used in our work.

Let{us}consider a multi-hop MANETs, where multiple-nodes are transmitting the information through an intermediate node say 'Z', which has energy capacity of 'E' joules which contain B bytes of buffer capacity with input queue 'Bi' with storage capacity of 'n_i' packets and output queue 'Bo' with storage capacity of 'no' packets. Packet arrive rate at input queue is 'Ra' and packet departure rate from output queue is 'Rd', and packet Processing rate of the node processor is 'R_p'. Packets 'P_i' (i=1,2,3,..) arrives the input queue at 'Tai' and leave from the queue at 'T_{di}', and arrives at output queue at 'T_{ao}' and leave from the queue at 'T_{do}'. Delay inside the input queue is 'T_{di}-T_{ai}' and output queue is 'T_{di}-T_{do}'

$$R_a = \frac{n_i * P}{T_{di} - T_{ai}}$$

$$R_p = \frac{n_p * P}{T_{pr}}$$

$$R_d = \frac{n_o * P}{T_{do} - T_{ao}}$$

There exist two synchronization constants K_1, K_2 can be defined as below equations.

$$K_1 = \frac{R_a}{R_p}$$

$$K_2 = \frac{R_p}{R_d}$$

Packet loss occur, If K_1>1then the packet arrives at input queue higher than its processing rate and if K_2>1then the packet departure rate from its output queue is less than its processing rate.

Table 1. Comparison between existing approach and proposed approach

Security Parameters	Existing	Proposed
Chebyshev Polynomial	No	Yes
ECC	Yes	No
RSA	Yes	No
XOR	Yes	Yes
Hash Function	Yes	Yes

Node has a energy of 'E' joules, and will take the E_r,E_p &E_t, joules of energy to receive, process and transmit the packet. Energy drain rate of a node to successfully process one packet is given by.

$$E_d = \frac{E_r + E_{p+}E_t}{E}$$

In a given time interval 'T' node can successfully process 'N_d' packets, and its drain rate will be

$$E_d = \frac{N_d*(E_r + E_{p+}E_t)}{E}$$

If packet arrive to node greater than the $N_d$limit in a time interval 'T' packet loss will occur.

In order to know the data processing capacity of an node of energy 'E' joules and drain rate of 'E_d' within a time interval 'T' ,We assume that in given number of data packets which needs to be process through node 'Z' in a network. We are using the Knapsack algorithm with n-Topples of positive values as

1. Number of data packets which need to process through the given nodelet Packets 'P_i'(i=1,2,3,..)
2. Energy drain rate and data rates consumed by the node to process the packet, include transmit, process and receive is given respectively as

$$R_a, R_p, \ R_a \text{ and } E_d$$

We need to determine the energy drain rate of packets in bytes K$\in$ {P_1,P_2 …P_n } to

Maximize ΣP_i where i K Subject to $\Sigma E_d(P_i) \leq E_d$

To get optimized data processed by an intermediate node for given energy capacity 'E' and drain rate of ' E_d', in a 'T' interval time. Possibility is to try for all 2 n possible subsets of 'K' to construct two dimensional arrays

$L[0\ldots..n,0\ldots.E_d]$ $1 \leq P_i \leq n \& 0 \leq E_d(P_i) \leq E_d$

Such that V [I,V] will process maximum data packets of any subset of flows with P_i packets of data{i=1,2,3,…..n}of energy drain rate required to process atmost 'E_d'. Array entries are L[n,E_d] will contain maximum data packets to process from given intermediate node. And array entries should not consider in below conditions.

1. $L[0,E_d]=0$ $0 \leq E_d(P_i) \leq E_d$ no datapacket process from the node
2. $L[i, E_d(P_i)] = -\infty \ \forall \ E_d(P_i) < 0$, illegal

Optimization solution is as follows

$L[I,E_d(P_i)] = \max(L[i-1, E_d(P_i)], L_i + L[i-1, E_d(P_i) - E_d(P_{i+1})]$

$1 \leq i \leq n$and $0 \leq E_d(P_i) \leq E_d$

To compute the actual subset, Knapsack adds an auxiliary Boole an array Keep[i,E_d (P_i)]which becomes one if node decide to process the P_i' the packet in V[i,E_d (P_i)]and it becomes zero otherwise. The algorithm m to calculate optimized data packet processing (DPP) by node is given below[37]

Algorithm

1. Knapsack(l,E_d (P_i),n,E_d){
2. for(E_d (P_i) =0toE_d) S[0,E_d (P_i)]=0;
3. for(i=1ton)
4. for(E_d (P_i) =0toE_d)
5. If((E_d (P_i) ≤E_d)and(l[i]+L[i-1,E_d-E_d (P_i)]> L[i-1,E_d (P_i)])){
6. L[i,E_d (P_i)]=l[i]+L[i-1, E_d-E_d (P_i)];
7. Keep[i,E_d (P_i)]=1; }
8. else V[i,E_d (P_i)]=L[i-1,E_d (P_i)];
9. Keep[i,E_d (P_i)]=0; }
10. K=E_d ;
11. for(I=ndownto1)
12. If(keep[i,K]==1){
13. Output i;
14. K=K-E_d (P_i) ;
15. Return L[n,E_d];

Algorithm1. Algorithm is to find the optimistic data packet processing capacity of node.

4. Cluster Formation

Clustering is the processes of dividing network into number of interconnected sub clusters. Clustering in network solve the issue of scalability and avoid expensive long distance communication and improve the availability of network resources by providing service locally and also better solution for key management problem. Every cluster contains a cluster head for co ordination purpose. Figure shows the proposed system model of network, in which mobile nodes divided into several clusters such a way that all the nodes are covered in clustering process and no node left. And moreover one node from each cluster elected as a cluster head to perform the functions of cluster coordination, key management and administration functions of cluster. Main aim of clustering in our approach is to avoid the single point of failure as clustering combines the both centralized and distributed approaches and limits the number of keys for secure communication and allow effective key management.

An effective clustering is one that divides the network into number of groups such a way that it preserves the network structure for long time. It depends up on selecting the cluster head, as failure of cluster head cause collapse of cluster. Cluster head majorly fail due to mobility, energy and heavy traffic and its constrained resources. In order to select an effective cluster head in MANETs environment, we consider two factors i.e, mobility and heterogeneity.

Mobility is one of the characteristic of MANETs which allow the nodes in a network to move freely. This affects the communication performance. Mobility is one of effective factor select cluster head, as moving cluster head cause the death of cluster members from cluster and increase the probability of cluster to collapse. Mobility of node is determined by 'V' and can be determined as.

$$V = \frac{\sqrt{\left(X_{t2} - X_{t1}\right)^2 + \left(Y_{t2} - Y_{t1}\right)^2}}{\hat{o}}$$

Where, $\hat{o} = \left(t_2 - t_1\right)$, node positions of at time t_1 is (X_{t1}, Y_{t1}) and nod e positions of at time t_2 is (X_{t2}, Y_{t2})

Heterogeneity: - Mobile devices can exist with different specifications and can directly affect communication performance of network. Different devices have different computation, storage, power, memory, disk, battery and communication capacities. Thus nodes in a network not only detect presence of neighbor nodes but also detect their attributes. The metric optimized data packet processing capacity of node addresses the heterogeneity.

Cluster based MANETs network architecture, Cluster head is the responsible for organization of cluster and should be in a better state with respect to resources (energy and processing capacities). We Calculated 'DPP' which is optimized data packet processing capacity of node is used to elect cluster head. Whenever network formed then all the nodes in a network need to run the algorithm to calculate their 'DPP' values. We are setting a threshold value DPP_{max}, is the value calculated by node under ideal conditions such as node with full of battery power and minimum traffic at inline queue of buffer. If nodes optimized packet process capacity greater than DPP_{max} with less mobility act as a cluster head. Remaining network construction is same as the existing work 'CHGSR'.

5. Analysis

In this section we analyze the network distribution with optimistic data packet processing capacity

1. Clustering in network solve the issue of scalability and avoid expensive long distance communication and improve the availability by providing service locally
1. Optimized packet processing capacity of node decide the nodes current condition with respect to its energy and traffic
1. Cluster head election based on metric Optimized packet processing capacity will increase the network life time[36]
1. Optimized packet processing capacity metric avoids the node to become bottleneck

6. Cluster based Authentication

In traditional public key architecture contain a fixed Registration Centre (RC), and then the network member uses the secure information from registration centre to authenticate and communicate with other network members. System is deepened on single node of setting and suffering from single point of failure, which compromises

the whole system security. MANETs require a distributed authentication model due to its distributed behaviour. In our proposed Cluster Based Mutual authenticated key agreement architecture, the registration centre is distributed among the cluster head, any cluster head can act as a RC. It is an overcome of single point of security problem. Our proposed work is based on Chebyshev polynomials, which is defined as follows

$\cos n\theta$ Can be written as polynomials in $\cos n\theta$ then[38,39]

$$\cos n\theta = T_n \cos\theta \quad (1)$$

$$\cos((n+1)\theta) = 2\cos(n\theta).\cos\theta - \cos((n-1)\theta)$$

$$T_{n+1}(\cos\theta) = 2T_n(\cos\theta)\cos\theta - T_{n-1}(\cos\theta)$$

$$T_{n+1}(X) = 2X\,T_n(X) - T_{n-1}(X) \quad (2)$$

Equation 2 represents the chebyshev polynomial $T_n(X)$ is a polynomial in 'X, degree 'n'.

In order to provide authentication work uses semi group property of Chebyshev polynomials as below

$$T_n(X) = (2X\,T_{n-1}(X) - T_{n-2}(X)) \pmod N \quad \ldots\ldots\ldots\ldots\ldots\ldots 3$$

Where $n \geq 2$ and N is a large prime number and X ϵ (-∞, +∞). In equation (3) given $T_n(X)$, X and N, it is mathematically infeasible to find the value of 'n', i.e, Chaotic Maps-Based Discrete Logarithm problem[25],

The composition property of Chebyshev polynomials states as follows,

$$T_n(T_m(X)) = T_m(T_n(X)) = T_{nm}(X) \quad \ldots\ldots\ldots 4$$

Where $m,n \geq 0$ and N is a large prime number andX ϵ (-∞, +∞). In equation (4) given $T_n(X), T_m(X)$,X and N, it is mathematically infeasible to find the value of $T_{nm}(X)$, i.e, Chaotic Maps Based Diffie-Hellman problem. The idea behind our work is come from equation (3,4).

7. Key Generation and Distribution

Our work is based on Chebyshev polynomials based cluster authentication architecture. Consider a Cluster based Mobile ad hoc network with cluster heads as Hi (i=1,2,3..) and respective cluster members of each cluster as Mi (i=1,2,3..)

1. All the nodes in MANETs assign with a unique identity i.e cluster heads as Hi i=1,2,3..) and cluster members as Mi (i=1,2,3..)

2. We assumes a trusted offline outside third party of network is decide the trusted one way hash function and symmetric cryptosystem of network

All the cluster head in a network let CH_i with identities ID_{chi} randomly select a large prime numbers X_i and K_i and compute the values of $T_{Ki}(X_i)$ based on Chaotic Maps-Based Discrete Logarithm problem from equation (3), where public information is (X_i, K_i, ID_{chi}, $T_{Ki}(Xi)$) and private information is 'K_i' .

All the member of cluster let CM_j with identities ID_{cmj} selects a large prime number K_j and compute the value of $T_{Kj}(_{Xi})$, where public information is (ID_{cmj}, $T_{Kj}(Xi)$).

3. Cluster head public information distributed to cluster members whenever cluster form and whenever new updates occur and to the newly joined cluster member.

4. Cluster member public information is send to cluster head whenever cluster member becomes source and when ever cluster head put request.

In order to provide strong authentication our scheme uses two keys i.e. Cluster key and session key. Whenever new node enters into cluster and detected by cluster head by means of hello message. Cluster head sends public information of cluster to cluster member including Identities, cluster head public key and common encryption and decryption algorithms. Node will calculate the cluster key with the help of public key of cluster head, and sends its public key to cluster head. Cluster key is used for authentication between cluster member and cluster head. Every node in a cluster must agree a cluster key with cluster head. Due to mobility node leaves the cluster and joins another cluster. The new cluster head treats the joining node as new node and therefore node and cluster head agree on cluster key shown in Figure 1. The old cluster removes the entry and its cluster key of the moved node after predefined time interval (when it does not receive the hello message from node).

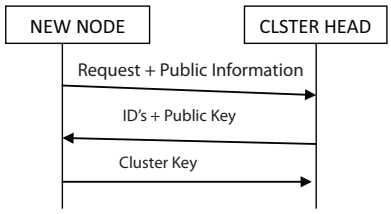

Figure 1. New node getting cluster key.

The session key is computed and shared between two communicating nodes with the help of cluster head and cluster keys therefore serves as authentication. In order provide complete confidentiality of information, the entire message has to be encrypted and decrypted by session key.

Algorithm

Consider a cluster with cluster head 'C' and mutual authentication and key agreement between cluster members 'A' and 'B'.Public information about the cluster is {X, P,ID_c, $T_c(X)$}, nodes are their Identities ($ID_{mi,}ID_a$,ID_b) and they agree on common encryption and decryption algorithm with secure hash function

Step1

Cluster node 'S' selects a random number's' and compute the values of $T_s(X)$ and $K_{sc} = T_s T_c(X)$ using its public information received from cluster head X, $T_c(X)$, and $H_s = \{ID_s xor ID_c xor ID_d xor T_s(X)\}$, $C_s = \{ID_s xor ID_c xor ID_d xor H_s\}$. Then source send the message $m_s = \{ID_s, ID_c, ID_d, T_s(X), C_s\}$ to the cluster head whereit wants to authenticated with node 'D'.

Step 2

Whenever cluster head 'C' receives the message $m_s = \{ID_s, ID_c, ID_d, T_s(X), C_s\}$ from cluster member, cluster head will calculate the secrete key $K_{sc} = T_s T_c(X)$ using the value of $T_s(X)$ from the message m_s. Using this K_{sc} it will decrypt the C_s and compute the value of H_s and check the H_s with the received H_s value in message m_s .if both matches then it conclude that node S is a valid participant. Then cluster head forward the request to node D for its public information with indicating that node S want to authenticate with you. And send the message as $m_c = \{ID_s, ID_c, ID_d, T_c(X),\}$

Step3

Cluster node 'D' selects a random number'd' and compute the values of $T_d(X)$ and $K_{dc} = T_d T_c(X)$ using its public information received from cluster head X, $T_c(X)$, and $H_d = \{ID_s xor ID_c xor ID_d xor T_d(X)\}$, $C_d = \{ID_s xor ID_c xor ID_d xor H_d\}$. Then source send the message $m_d = \{ID_s, ID_c, ID_d, T_d(X), C_d\}$ to the cluster head

Step 4

After receiving the response message $m_d = \{ID_s, ID_c, ID_d, T_d(X), C_s\}$ from cluster member 'D' , cluster head will calculate the secrete key $K_{dc} = T_d T_c(X)$ using the value of $T_d(X)$ from the message m_d. Using this K_{dc} it will decrypt the C_d and compute the value of H_d and check the H_d with the received H_d value in message m_d .if both matches then it conclude that node 'D' is a valid participant. Then cluster head computes the session key $K_{sd} = T_s T_d(X)$ with the help of public information received from nodes 'S' and 'D' such as $T_d(X), T_s(X)$.

Step 5

Cluster head forward the session key securely to nodes D and S by encrypting with its long secrete keys. Massage $m_{cs} = K_{sc}\{K_{sd}\}$ to node S and message $m_{cd} = K_{dc}\{K_{sd}\}$ to node D

Step 6

Nodes S and D decrypt the messages m_{cs} and m_{cd} using their long secrete key respectively and retrieve the session key K_{sd}. Now all the messages are encrypted between 'S' and 'D' with session key. Figure 2 describe the above algorithm

8. Performance Calculations

Chaotic Maps based cryptography is one of the four cryptographic systems presently used in public key infrastructure; the remaining three systems are integer factorizations, elliptic curve and discrete logarithms. The RSA cryptography system is the well known example of integer factorization system, The Digital Signature algorithm systems are the best example of discrete logarithm. Elliptic curve cryptography systems are based on elliptic curve and effective public key cryptography system for wireless network environment than RSA. In comparison with RSA, ECC allows faster computation, smaller key

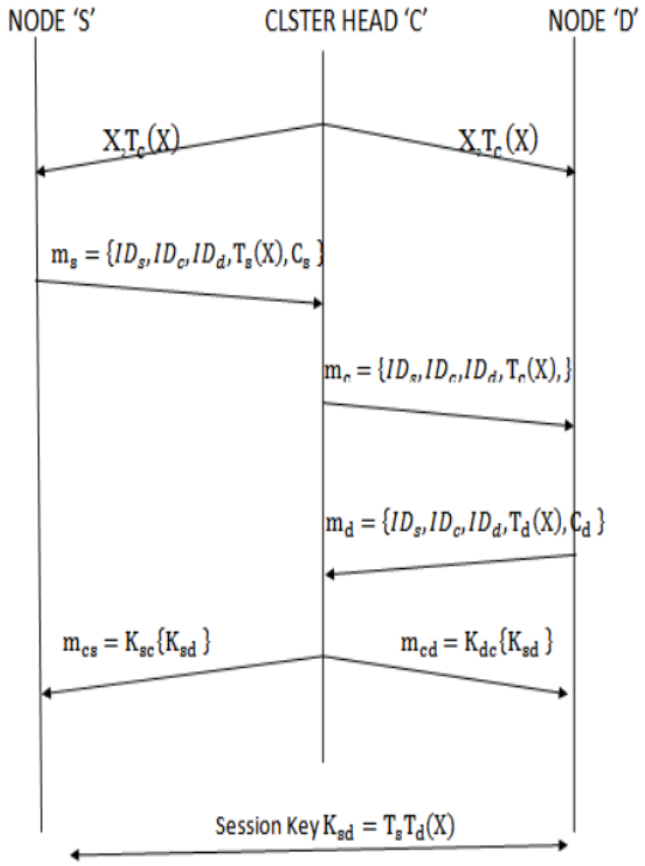

Figure 2. Authenticated key agreement algorithm.

and equal security {reference}.Compare to ECC and RSA, Chebyshev polynomial computing offers small key size, faster computation, and energy, memory, bandwidth saving.

We compare our work with existing[40] proposed an "An ECC-Based Key agreement Protocol for MANETs", which is designed for two party authenticated key agreement, and authors gives detailed comparison with existing four key agreement protocols with respect to computational overhead, and demonstrated that the proposed model is efficient. Thus in this section, we only compare our scheme with existing[40]model. Since MANET is heterogeneous network with constrained resources, power consumption is always a big issue and it is not easy to measure[41]. Thus we used the primitive operation count to evaluate the computation cost for performance calculation at nodes, which participate in key agreement. Notation Used for Computation Cost is as below

1. T_{cheb} denotes the executing time for the Chebyshev polynomial computing.

2. T_{Ecc} denotes the executing time for the elliptic curve point multiplication.

Compare to ECC and RSA, Chebyshev polynomial computing offers small key size, faster computation, and energy, memory, bandwidth saving. More than that ECC offer computation overhead by scalar multiplication and modular exponentiation. Hongfeng Zhu mentioned that Chebyshev polynomial executing time(T_{cheb}) operation is computationally 0.042055 s faster than elliptic curve point multiplication executing time(T_{Ecc})operation in same resources and network environment. It could be clear from Table1 our model is cost effective in terms of time complexity with existing approach.

9. Security Analysis

Security analysis of proposed protocol is as fallows,

1. We have used the security component based on Chaotic Maps Based Diffie Hellman problem, Chaotic Maps-Based Discrete Logarithm problem for calculation of cluster key and session key, which could not be possible to solve in polynomial time.

2. Assuming that the attacker has full control to enter on to the network to perform malicious activities through insecure channel. However, attacker could not get the knowledge to compute the session and cluster keys.

3. Compare to the key generation algorithms such as RSA & ECC, our algorithm offers smaller key size, faster computation, memory and energy saving therefore well suited for MANETs characteristics.

4. Session key generated on reactively and no information is stored in network, thus our model is resist against stolen verification attack and modification attack.

5. Nodes can change the cluster key and update the cluster key, thus our model resist against guessing attack.

Session key security:- Session key agree between sender and destination node is protected from other nodes by cluster key. Session key in our method calculated by cluster head as $K_{sd} = T_s T_d(X)$, where the values of s, and d are different in different sessions , and session key is send to particular node by encrypting nodes cluster key.

Mutual authentication:- The aim of mutual authentication is to conform two communicating nodes in a network to authenticated each other and simultaneously agree on a common session key. In our approach two communicating nodes authenticated by cluster head by checking the value of H_s and H_d. And both agree on a common session key K_{sd}, where intended nodes only retrieve the session key as it is encrypted by long secrete key of particular node shown in step 4 of key agreement phase.

Key freshness. :- key freshness property increase the security of communication session by providing new and updated keys. In our method the values of X, $T_c(X)$, $T_s(X)$, $T_d(X)$ are changed in every session. Thus the session key also change ,which causes the cryptanalytic attack much difficult

1. Efficiency:-The key management service in our approach is efficient with respect to communication, computational, memory, and energy resources compare with ECC and RSA.

2. Resistance to tamper attack :- it is a attempt by attacker to modify or change the information in an unauthorized way

10. Conclusion

In this work, we introduced an "Energy aware Mutual authenticated key agreement scheme" for MANETs. As MANETs is infrastructure less, we avoided centralized architecture for implementing key management. We considered cluster based network & selection of cluster head is based on metric called optimized data packet processing capacity with respect to current traffic & residual energy, which improves the lifetime of network and to avoid the node to become bottleneck. Moreover Cluster head generate, maintain, and distribute the keys in their cluster in a secure manner. Our concept uses Chebyshev polynomials to provide mutual authenticated key agreement, which assures that the session key is established only between two intended entities. Moreover our method needs less computational overhead compared with RSA and ECC and well suitable for MAETs environment.

11. References

1. Mohammad AAK, Sharifi A, Sharifi H. Secured-Bandwidth Reservation Distance Vector Routing Protocol. International Journal of Scientific Research in Computer Science Applications and Management Studies. 2012; 1(3):1–4.
2. Sasila Jabamani S, Rajinikanth E. Integrity Key based Mechanism to Debase Packet Dropping in Manets. Indian Journal of Science and Technology. 2016 Apr; 9(14). Doi:10.17485/ijst/2016/v9i14/90204.
3. Muthuramalingam S, Suba Nachiar T. Enhancing the Security for Manet by Identifying Untrusted Nodes using Uncertainity Rules. Indian Journal of Science and Technology. 2016 Jan; 9(4). Doi:10.17485/ijst/2016/v9i4/87043.
4. Jesudoss A, Subramaniam NP. EAM: Architecting Efficient Authentication Model for Internet Security using Image-based One Time Password Technique. Indian Journal of Science and Technology. 2016 Feb; 9(7). Doi:10.17485/ijst/2016/v9i7/85017.
5. Rafidha Rehiman KA, Veni S. A Secure Authentication Infrastructure for IoT Enabled Smart Mobile Devices – An Initial Prototype. Indian Journal of Science and Technology. 2016 Mar; 9(9). Doi:10.17485/ijst/2016/v9i9/86791.
6. Vijayakumar K, Somasundaram K. Study on Reliable and Secure Routing Protocols on Manet. Indian Journal of Science and Technology. 2016 Apr; 9(14). Doi:10.17485/ijst/2016/v9i14/84433.
7. Gautam S, Kumar R. A Review of Energy-Aware Routing Protocols in MANETs. International Journal of Modern Engineering Research (IJMER). 2012; 2(3):1129–33.
8. Babu KS, Chandra K, Sekharaiah. Securing AODV with Authentication Mechanism Using Cryptographic Pair of Keys. International Journal of Computer Science and Information Security. 2013; 11(2):42–5.
9. Rafaeli S, Hutchison D. A survey of key management for secure group communication. ACM Computing Surveys (CSUR). 2003; 35(3):309–29.
10. Wang N-C, Fang S-Z. A hierarchical key management scheme for secure group communications in mobile ad hoc networks. Journal of Systems and Software. 2007; 80(10):1667–77.
11. Kim Y, Perrig A, Tsudik G. Simple and fault-tolerant key agreement for dynamic collaborative groups. Proceedings of the 7th ACM Conference on Computer and Communications Security. ACM. 2000. p. 235–44.
12. Ateniese G, Steiner M, Tsudik G. Authenticated group key agreement and friends. Proceedings of the 5th ACM Conference on Computer and Communications Security. ACM. 1998. p. 17–26.
13. Burmester M, Desmedt YG. Efficient and secure conference-key distribution. Security Protocols. Springer-Veralg: Berlin Heidelberg. 1997; 119–29.
14. Blom R. An optimal class of symmetric key generation systems. Advances in cryptology. Springer-Verlag: Berlin Heidelberg. 1985; 335–38.
15. Blundo C, et al. Perfectly secure key distribution for dynamic conferences. Information and Computation.1998; 146(1):1–23.
16. Jambhekar D, Dhawale CA. Bit Level Key Agreement and Exchange Protocol for Digital Image Steganography. Indian Journal of Science and Technology. 2015 Jul; 8(15). Doi:10.17485/ijst/2015/v8i15/70915
17. Wang X-Y, Chen F, Wang T. A new compound mode of confusion and diffusion for block encryption of image based on chaos. Communications in Nonlinear Science Numerical Simulation. 2010; 15(9):2479–85.

18. Li C, Li S, Alvarez G, Chen G, Lo K-T. Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations. Physics Letters A. 2007; 369(1–2):23–30.
19. Bose R. Novel public key encryption technique based on multiple chaotic systems. Phys Rev Lett. 2005 Sep; 95(9):098702.
20. Kocarev L, Tasev Z. Public-key encryption based on Chebyshev maps. Proceedings of the IEEE 2003 International symposium on Circuits and Systems. 2003; 3:28–31.
21. Xiao D, Shih FY, Liao X. A chaos-based hash function with both modification detection and localization capabilities. Communications in Nonlinear Science Numerical Simulation. 2010; 15(9):2254–61
22. Amin M, Faragallah OS, Abd El-Latif AA. Chaos-based hash function (CBHF) for cryptographic applications. Chaos, Soliton Fractls. 2009; 42(2):767–72.
23. Wang X, Zhao J. An improved key agreement protocol based on chaos. Commun Nonlinear Science Numerical Simulation. 2010; 15(12):4052–57.
24. Yoon E, Jeon I. An efficient and secure Diffie–Hellman key agreement protocol based on Chebyshev chaotic map. Communications in Nonlinear Science Numerical Simulation. 2011; 16(6):2383–89 .
25. Lai H, et al. Applying semigroup property of enhanced Chebyshev polynomials to anonymous authentication protocol. Mathematical Problems in Engineering. 2012; 17.
26. Zhao F, Gong P, Li S, Li M, Li P. Cryptanalysis and improvement of a three-party key agreement protocol using enhanced Chebyshev polynomials. Nonlinear Dynamics. 2013; 74(1):419–27.
27. Ozkaynak F, Yavuz S. Designing chaotic S-boxes based on time-delay chaotic system. Nonlinear Dynamics. 2013; 74(3):551–57.
28. Alvarez G. Security problems with a chaos-based deniable authentication scheme. Chaos Solitons Fractals. 2005; 26(1):7–11.
29. Xiao D, Liao X, Deng S. A novel key agreement protocol based on chaotic maps. Information Sciences. 2007; 177(4):1136–42 .
30. Han S. Security of a key agreement protocol based on chaotic maps. Chaos Solitons Fractals. 2008; 38(3):764–68.
31. Chiang, C-C, Wu H-K, Liu W, Gerla M. Routing in clustered multihop, mobile wireless networks with fading channel. In proceedings of IEEE SICON. 1997; 97(4):197–211.
32. Mason JC. Handscomb D C. Chebyshev polynomials. CRC Press: USA, 2002.
33. Zhu H. Flexible and Password-Authenticated Key Agreement Scheme Based on Chaotic Maps for Multiple Servers to Server Architecture. Wireless Personal Communications. 2015; 82(3):1697–718.
34. Zhen P, et al. Key agreement protocol based on extended chaotic maps with anonymous authentication. Chaotic Modelling and Simulation (CMSIM0). 2014; 3(3):221–31
35. Cai Z, et al. A Chebyshev-Map Based One-Way Authentication and Key Agreement Scheme for Multi-Server Environment. International Journal of Security and its Applications. 2015; 9(6):147–56.
36. Mohammad AAK, Mirza A, Razzak MA. Reactive Energy Aware Routing Selection Based on Knapsack Algorithm (RER-SK). In Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI, Springer International Publishing: Switzerland, 2015; 289–98.
37. Martello, S, Toth P. Knapsack Problems, J. 1990.
38. Wang X, Zhao J. An improved key agreement protocol based on chaos. Communications in Nonlinear Science Numerical Simulation. 2010; 15(12):4052–57.
39. Yoon EJ, Jeon I. An efficient and secure Diffie–Hellman key agreement protocol based on Chebyshevchaotic map. Communications in Nonlinear Science Numerical Simulation. 2011; 16(6):2383–89.
40. Ammayappan K, et al. An ECC-based two-party authenticated key agreement protocol for mobile Ad Hoc networks. Journal of Computers. 2011; 6(11):2408–16.
41. Chai Z, Cao Z, Lu R. Threshold password authentication against guessing attacks in Ad hoc networks. Ad Hoc Networks. 2007; 5(7):1046–54.