Journal of Theoretical and Applied Information Technology
31st August 2017. Vol.95. No.16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN OPTIMAL KEY MANAGEMENT TECHNIQUE FOR SECURE DATA TRANSMISSION IN MANET

[1]M. ANUPAMA, [2]DR. B. SATHYANARAYANA

[1]Associate Professor, MVSR Engineering College, Department of Computer Science and Engineering, Hyderabad, India

[2]Professor, Sri Krishnadevaraya University, Department of Computer Science and Technology, India

E-mail: [1]anu_meduri@yahoo.co.in, [2]bachalasatya@yahoo.com

ABSTRACT

Cryptographic techniques are commonly used for secure data transmission in wireless networks. Most cryptographic techniques, such as symmetric and asymmetric cryptography, often involve the use of cryptographic keys. Key management is one of the vital aspects of security in mobile ad hoc networks. In mobile ad hoc networks, the processing load and complexity of key management are strongly subject to restriction by the node's available resources like energy and the dynamic nature of network topology. The Key Management technique is proposed which uses symmetric key management. The distribution of keys in an authenticated manner is a difficult task in MANET. In this paper, we have proposed a secure and optimal key management system in MANET. Initially the mobile input nodes are selected with the aid of soft computing technique. The nodes are clustered by using Fuzzy C-means (FCM) clustering algorithm. The clustered nodes are then optimized in order to select the exact amount of nodes for communication. This optimization can be performed with the aid of Enhanced Bacterial Foraging Optimization (EBFO) technique. We use this for authenticating and key sharing to forward security parameters in a novel and secure way. For authentication, we will use the Elliptic Curve Deffie-Hellman (ECDH). This key exchange scheme shares a symmetric key among parties, which is necessary to have a low cost confidentiality in upcoming communications. This delivers a minimum overhead on the network by using ECDH.

Keywords: *Cryptography, Key Management, MANET, Fuzzy C-means clustering, Enhanced Bacterial foraging, Elliptic Curve Deffie-Hellman.*

1. INTRODUCTION

The number of applications available for wireless communications is growing rapidly: mobile telephony is ubiquitous nowadays, wireless hotspots are spreading everywhere, and also ad hoc networking is growing mature these days. A key characteristic of these scenarios is the dynamic behavior of the involved communication partners. Communication protocols will have to deal with a frequently changing network topology. However, many applications require stable connections to guarantee a certain degree of QoS [1]. Mobile Ad Hoc networks are attractive for a wide variety of applications, such as battlefield surveillance and emergency response. These networks are prone to losses due to wireless medium, mobility, fading, misbehaving nodes, etc. Transport protocols for mobile ad hoc networks must address these issues to achieve better performance [5]. Ad hoc network is a particular wireless mobile network, which is characterized by multi-hop routing and dynamic topology. In such networks, selecting stable routes is essential for QoS provisioning. A route includes a sequence of links. Even if only one link in the sequence fails, the route no longer works. That is, route stability is heavily affected by link stability. Thus, selecting stable links can reduce rerouting times and lengthen the lifetime of routes effectively [2]. The performance of a mobile ad hoc wireless network is impacted by the dynamic stochastic process characteristics of its underlying links, nodes, the underlying graph connectivity of the network topology, and the application induced traffic loading processes and their required quality of service (QoS) objectives. Under typical on-demand ad hoc routing algorithms, a source node that wishes to communicate across the network, initiates a route discovery process [3]. Understanding node mobility is one of the keys to determine the potential capacity of an ad hoc network. Various mobility metrics have been proposed as measures of topological change in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

networks. Metrics describing the link or path stability allow adaptive routing in MANETs based on predicted link behavior [4].

Network resources such as bandwidth and power have to be dealt with in fundamentally different ways compared to wired or centralized cellular networks. Resource availability can quickly change, and therefore, continuous resource reallocation is needed to provide graceful degradation during overloads or quality-of-service (QoS) improvements when more resources become available [6]. A mobility model is one of the most important components in the simulation of MANETs. This component describes the movement pattern of mobile nodes, impacting on protocol performance, topology and network connectivity, data replication, and security. The performance of a protocol can vary dramatically depending on the adopted mobility model. Mobility models can be classified into four categories: random, temporal-based, spatial-based (or group-based), and with geographic restriction [7]. Routing and MAC protocols that exploit fading channel-state-information (CSI) at the transmitter have the potential to improve upon conventional routing protocols and have attracted the attention of researchers [8]. In this paper, Optimal Key Management for secure Data transmission (OKMSDT) is proposed. The mobile input nodes are clustered by using Fuzzy C-means (FCM) clustering algorithm. These clustered nodes are optimized by using EBFO in order to select the exact amount of nodes for communication. For secure communication of mobile input nodes ECDH technique is employed. The encryption and cluster formation algorithms are providing security to messages contained in the nodes.

2. RELATED WORK

Numerous researches have been done in the field of MANET for improving the mobility metrics. Some of the recent researches done in the field of MANET are given below,

Curescu et al. [9] proposed a scheme for bandwidth allocation in wireless ad hoc networks. The quality-of-service (QoS) levels for each end-to-end flow was expressed using a resource-utility function, and their algorithms aimed to maximize aggregated utility. The shared channel was modeled as a bandwidth resource defined by maximal cliques of mutual interfering links. They proposed resource allocation algorithm that employs an auction mechanism in which flows are bidding for resources. The bids depend both on the flow's utility function and the intrinsically derived shadow prices. They then combined the admission control scheme with a utility aware on-demand shortest path routing algorithm where shadow prices are used as a natural distance metric. But, during the simulation to packet drop and retransmission still improvement required.

Leng et al. [10] have presented k-hop Compound Metric Based Clustering (KCMBC) scheme, which uses the host connectivity and host mobility jointly to select cluster-heads. KCMBC was a fast convergent and load balancing clustering approach that was able to offer significant improvement on scalability for large-scale ad hoc networks. On the other hand, since host mobility has been taken into account in terms of the average link expiration time, the clusters constructed by KCMBC are more stable than many other schemes. The control overheads for cluster formation using the KCMBC scheme are kept relatively low if compared to other clustering schemes. The proposed scheme increased the cluster head life time, but more energy consumption occurs for clustering. This will decrease the overall network stability in ad hoc wireless networks.

A mobile ad hoc network is collection of self-configuring and adaption of wireless link between communicating devices (mobile devices) to form an arbitrary topology and multihop wireless connectivity without the use of existing infrastructure. It requires efficient dynamic routing protocol to determine the routes subsequent to a set of rules that enables two or more devices to communicate with each other's. Santosh et al. [11] have classified and evaluated the mobility metrics into two categories- direct mobility metrics and derived mobility metrics. These two mobility metrics had been used to measure different mobility models, also considers some of mobility models i.e. Random Waypoint Model, Reference Point Group Mobility Model, Random Direction Mobility Model, Random Walk Mobility Model, Probabilistic Random Walk, Gauss Markov, Column Mobility Model, Nomadic Community Mobility Model and Manhattan Grid Model. Here, mobility model classified based on direct and derived metric. Classification improvement still required based on routing protocol performance.

Zhang., et al. [12] have analyzed the effect of mobility on information spreading in geometric networks through natural random walks. Specifically, their focus was on epidemic propagation via mobile gossip, a variation from its static counterpart. Their contributions are twofold. Firstly, they proposed a performance metric, mobile

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

conductance, which allows to separate the details of mobility models of mobile spreading time. Secondly, they utilized geometrical properties to explore this metric for several popular mobility models, and offer insights on the corresponding results. Large scale network simulation was conducted to verify their analysis. Here, only consider the single piece data dissemination through a natural randomized gossip algorithm but multi piece data not performed.

In highly mobile networks, mobility based clustering schemes exploit the group mobility of nodes to form stable communication structure by grouping nodes with similar mobility pattern together. However, existing group mobility metrics could not assess quantitatively whether a mobility model could provide the necessary degree of group mobility. Xia and Yeo [13] have proposed a metric, Degree of Node Reachability (DNR), to measure the degree of group mobility from the perspective of network topology. Based on DNR, they proposed r-test to quantitatively assess whether a given mobility model would fail to satisfy the required network condition. The proposed metric was validated using common mobility models. Here, only measures of the degree of group mobility from network but security between nodes are still improved.

Reina., et al. [14] proposed hybrid broadcast scheme for mobile wireless networks. The main objective was to combine different flooding schemes in order to solve the broadcast storm issue encountered by the simple flooding scheme. For this purpose, the density of nodes was taken into account using a density metric called expansion metric. In addition, in order to reduce the broken links due to mobility of nodes and increasing dissimilarity among the intermediate nodes, a forwarding zone criterion was included in the proposed schemes. The proposed approaches have been implemented and compared with pure probabilistic flooding, and simple flooding schemes. The hybrid flooding scheme reduces the overhead caused by the broken links but this technique is costlier in terms of bandwidth.

Jin-Hee Cho., et al. [15] developed a mathematical model for analyzing scalable region-based hierarchical group key management protocol integrated with intrusion detection to handle both outsider and insider security attacks for group communication systems (GCSs) in mobile ad hoc networks (MANETs). The proposed adaptive intrusion detection technique relied on majority voting by nodes in a geographical region to cope with collusion of compromised nodes, with each node preloaded with anomaly-based or misuse-based intrusion detection techniques to diagnose compromised nodes in the same region. The hierarchical group key management of adaptive intrusion was detected by mobile nodes in homogenous environment but in heterogeneous not suitable.

Dijiang Huang., et al. [16] presented a secure group key management scheme for hierarchical mobile ad-hoc networks to enhance both scalability and survivability of group key management for large-scale wireless ad-hoc networks. The scheme proposed a multi-level security model, and a decentralized group key management infrastructure to achieve such a multi-level security model. These approaches minimized the key management overhead and improved resilience to any single point failure problem. A roaming protocol was proposed to provide secure group communication involving group members from different groups without requiring new keys. However, with the increases in the number of groups and the height of the hierarchical structure, the communication overhead and the key derivative complexity do increase. Here, Bell-La Padula security model was employed in hierarchical mobile ad-hoc network. This model of security levels of objects being statics.

Xingwen Zhao., et al. [17] presented a generic construction of dynamic asymmetric group key agreement (DASGKA) by combining a conventional authenticated group key agreement, a public key encryption and a multi-signature. After computing a shared private key, a corresponding public key was published to outsiders. A multi-signature was attached as a trust for public key. The construction maintained the advantage of asymmetric group key agreement, and enabled users to join or leave the group efficiently without triggering a completely new key agreement protocol, which will greatly benefit the users in ad hoc networks. The proposed protocol was employed in group communication, group key shared by all group members. So, the security between each group communication is low in an ad hoc network.

Jin-Hee Choa., et al. [18] proposed and analyzed a scalable and efficient region-based group key management protocol for secure group communications in mobile ad hoc networks. A region-based approach was presented for scalability and dynamic reconfigurability by which group members are broken into region-based subgroups. Leaders in subgroups securely communicate with

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

each other to agree on a group key with respect to membership change and member mobility-induced events. An approach was proposed for identifying the optimal setting of the region-based key management protocol to maximize the performance of the system. The proposed system concentrated only on secure communication in mobile ad hoc network but energy consumption issue was raised. Nodes in ad hoc network rely on their power sources and CPU take more time and energy.

Yanji Piao., et al. [19] presented group key generation for intra-group communication and focused on the polynomial generation for creating secure inter-group key. The proposed scheme allowed group members and group controllers to share the intra-group key without any encryption/decryption. These mechanisms could reduce the number of re-keying messages during group changes using the polynomial. The polynomial based key generation was provided more security of group communication but, computation rate was more due to if each node joins or leaves in operation in that situation polynomials were regenerated and key was refreshed.

Jen-Chiun Lin., et al. [20] proposed a group key management protocol to reduce the communication and computation overhead of group key rekeying due to membership changes. The shared key derivation denied server to encrypt or decrypt the keys derivable by members themselves and the performance of synchronous and asynchronous rekeying operations, including single join, single leave, and batch update, was thus improved. The proposed protocol was secure and immune to collusion attacks. Here, group key management protocol was operating in a multi-level environment. While performing among groups' privacy and security improvement still required.

3. PROBLEM DEFINITION

Mobile networks are receiving an increasing research interest recently. Mobile ad hoc networks (MANET) and Vehicular ad hoc networks (VANET) are two prominent examples. In many real world networks, an interesting application is to broadcast the information from some source node to the whole network. For wireless ad hoc and sensor networks, a node triggered by the event of interest may want to inform the whole network about the situation as quickly as possible.

- Effect on information spreading is still not efficient.
- The information spreading speeds up or slows down effectiveness.
- Quantify the potential improvement or degradation due to mobility.
- A trust based clustering scheme was proposed to enforce authentication to the data [8]. Total trust degree and partial trust were estimated based on which cluster head was elected. Each node is updated with the trust relationship and according to which, a cluster can be broken, new cluster head can be elected etc.
- However, without encryption and decryption, security requirement could not be fulfilled.
- Security features including confidentiality, integrity, authentication, freshness, and non-repudiation are the major issues in MANET.
- The secured routing integrated framework is only concentrating on key management system [21]. Security is the major issue.

Hence we propose to develop a trust based clustering and group key management for secure communications in MANET.

Journal of Theoretical and Applied Information Technology
31st August 2017. Vol.95. No.16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

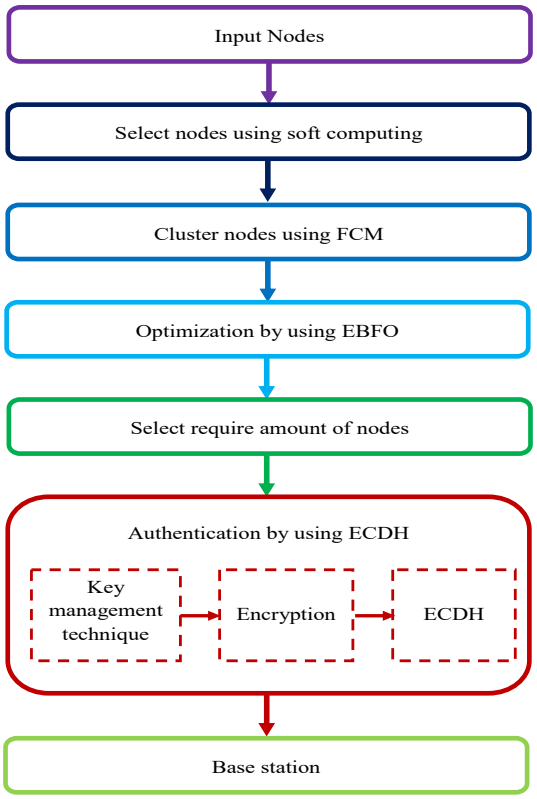

Figure 1: Proposed optimal Key management for secure data transfer

4. PROPOSED METHODOLOGY

In general, secure data transmission can be attained by encryption and decryption techniques. To achieve this, encryption keys are distributed to the nodes in the network. Distributing keys securely in the network is a critical task. The progression of key management involves key setup, the initial distribution of keys, and key revocation the removal of a compromised key. In this paper, the optimal key management system based on cryptographic and clustering algorithms are proposed. The soft computing technique is utilized for the selection of nodes in order to provide accurate means for capturing the spatial temporal dependence. The nodes are clustered using modified Fuzzy C means (FCM) algorithm. The clustered nodes are then optimized in order to select the exact amount of nodes required for communication by using EBFO algorithm. The ECDH key exchange scheme is employed for secure communication among nodes. This scheme shares a symmetric key among parties, which is necessary to have a low cost confidentiality in upcoming communication. This delivers a minimum overhead on the network by using ECDH. The implementation is done in NS2 platform and the performance will be analyzed with various networking attacks.

4.1 Fuzzy C-Means Clustering

The basic idea of this section is to reduce a required amount of nodes for communication through which the data can be transferred.

Step1: Subset formation

The FCM algorithm assigns cluster centre to each category by using fuzzy memberships.

$$J_m = \sum_{i=1}^{I}\sum_{j=1}^{J}(\mu_{ij})^m \left\|x_i - z_j\right\|^2 \quad (1)$$

In Eqn. (1), x_i represents the features $t(w(s_n^i))$, $c(s_n^i)$ extracted from the input database, z_j is the j th cluster centre and m is the constant value.

The membership function represents the probability that a cluster center belongs to a specific cluster. In the FCM algorithm, the probability is dependent on the distance between the pixel and each individual cluster center in the feature domain. The membership functions and cluster centers are updated by the equations (2) and (4).

$$u_{ij} = \frac{1}{\sum_{k=1}^{J}\left(\frac{\left\|x_i - z_j\right\|}{\left\|x_i - z_k\right\|}\right)^{\frac{2}{m-1}}} \quad (2)$$

Repeat the algorithm until the coefficients' change between two iterations is no more than ξ, for the given sensitivity threshold.

$$\max_{ij}\left\|U_{ij}^{(k)} - U_{ij}^{(k+1)}\right\| < \xi \quad (3)$$

In equation (3), ξ is a termination criterion between 0 and 1, whereas k are the iteration steps. The clusters centroid values are computed by using the equation (4).

$$z_j = \frac{\sum_{i=1}^{I} u_{ij}^m . x_i}{\sum_{i=1}^{I} u_{ij}^m} \quad (4)$$

To enhance the performance of the fuzzy-C-means clustering method, adaptiveness is invoked by measuring the Clustering effectiveness (α) and Absolute density (β). On the basis of these two, we set two thresholds to ensure the clustering being

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

good. After the FCM process, we obtain the number of cluster set such as $I_1, I_2, I_3, ..., I_n$. This clustered dataset is used for the further processing.

Step 2: Attribute selection

After the clustering process using FCM, we have to do the attribute selection process. Here, we calculate the minimum $A_{\min}$ and maximum $A_{\max}$ value of each column (or each attribute) in the dataset D_1 and D_2. If the $A_{\min}$ and $A_{\max}$ value is similar to corresponding dataset I_1 and I_2, we have to neglect that column.

Step 3: Discretization

Discretization is a significant step in data processing to convert the data into specific interval, means that the range of values is confined into a specific interval. Here, we have used one discretization function based on the predictable way. We perform the discretization process at first, we identify the maximum and minimum values of every attribute, and the K interval is tracked by taking the ratio between the deviated value and the K value.

$$for\ each\ "\ j"\ Dev^j = \left\lceil \frac{\max\left(A_j\right) - \min\left(A_j\right)}{3} \right\rceil$$

$$D^L = \min\left(A_j\right) \le \left[\min\left(A_j\right) + Dev^j \right] \quad (5)$$

$$D^M = \left[\min\left(A_j\right) + Dev^j \right] \le \left[\min\left(A_j\right) + 2 \bullet Dev^j \right]$$

$$D^H = \left[\min\left(A_j\right) + 2 \bullet Dev^j \right] \le \max\left(A_j\right) j$$

Using equation (6) we can adjust all the feature values in the specific interval. Now we obtain the new feature values, which feature values varies from specific interval. Then; every value that comes under within the range is replaced with the interval value so that the input data is transformed to the discretized data. Consequently, the training dataset D^{TR} is concerted to the discretized format D^D where, the entire data element D^D contains only the L, M, and H *if* $k = 3$.

Bacteria foraging optimization (BFO) algorithm is a new division of metaheuristic algorithm. It is a population-based optimization technique developed by inspiring the foraging manners of E. coli bacteria [12]. The basic operations of BFO algorithm is briefly discussed below.

4.2 Bacterial Foraging Optimization

Bacteria foraging optimization (BFO) algorithm is a new division of metaheuristic algorithm. It is a population-based optimization technique developed by inspiring the foraging manners of E. coli bacteria. The basic operations of BFO algorithm is briefly discussed below. Chemotaxis during foraging operation (tracing, handling, and ingesting food), an E. Coli bacterium moves towards the food location with the aid of swimming and tumbling by using flagella. Through swimming, it can move in a specified direction and during tumbling action, the bacteria can modify the direction of search. These two modes of operations are continuously executed to move in random paths to find adequate amount of positive nutrient gradient. These operations are performed in its whole lifetime.

Swarming

In this process, after the success in the direction of the best food position, the bacterium which has the knowledge about the optimum path to the food source will attempt to communicate to other bacteria by using an attraction signal. The signal communication between cells in E. coli bacteria is represented by the following equation:

$$J(\theta, D(j,k,l)) = \sum_{i=1}^{N} J_{cc}(\theta, \theta^j(j,k,l)) = A + B \quad (6)$$

$$A = \sum_{i=1}^{N} \left[-d_{attract} \exp(-W_{attract} \sum_{m=1}^{D} (\theta_m - \theta_m^i)^2) \right] \quad (7)$$

$$B = \sum_{i=1}^{N} \left[h_{repell} \exp(-W_{repell} \sum_{m=1}^{D} (\theta_m - \theta_m^i)^2) \right] \quad (8)$$

Where is the location of the global optimum bacterium till the jth chemotactic, kth reproduction, and lth elimination stage and "" is the mth parameter of global optimum bacteria.

Where $J(\theta, D(j,k,l))$ represents objective function assessment, "N" is the total numbers of bacterium and "D" the total parameters to be optimized. The other parameters such as $d_{attract}$ are the depth of attractant signal released by bacteria and $W_{attract}$ is the width of attractant signal. The signals h_{repell} and W_{repell} are the height and width of repellent signals between bacterium (attractant is the signal for food source and repellent is the signal for noxious reserve).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Reproduction

In swarming process, the bacteria build up as groups in the positive nutrient gradient and which may increase the bacterial concentration. After the congregation the bacteria are sorted in descending order based on its health values. The bacteria which have the least health will perish and the bacteria with the most health value will split into two and breed to maintain a constant population.

Elimination-Dispersal

Based on the environmental conditions such as change in temperature, noxious surroundings, and accessibility of food, the population of a bacteria may change either steadily or abruptly. During this stage, a group of the bacteria in a restricted region (local optima) will be eliminated or a group may be scattered (dispersed) into a new food location in the "D" dimensional search space. The dispersal possibly flattens the chemotaxis advancement. After dispersal, sometimes the bacteria may be placed near the good nutrient source and it may support the chemo-taxis, to identify the availability of other food sources. The above procedures are repeated until the optimized solutions are achieved.

4.3 Enhanced Bacterial Foraging Optimization (EBFO) Algorithm

The parameters of the basic BFO algorithms are defined in the following. D: the dimension of search space (the search boundary is $-100 < 0 < +100$), N: the total number of artificial E. coli bacteria, Nc: total number of chemo-taxis steps, Ns: swim length during the search, Nre: total number of reproduction steps, Ned: total number of elimination-dispersal events, Nr : number of reproduced bacteria, ped : the probability that each bacterium will be eliminated/dispersed, and n: the run length.

In the basic BFO algorithm, the fitness of each bacterium is determined from the average value of the entire chemo-tactic performance index before the reproduction operation. In the proposed EBFO algorithm, the bacterium with the maximum health is retained.

The health of the bacterium can be found by the following relation.

$$J^{i}_{health} = \sum_{j=1}^{N_c+1} j(i, j, k, l)$$

Where,

In the proposed algorithm, the retained bacterium is used to guide the reproduced bacteria towards the nutrient source. Due to this process, along with the accuracy in optimization, the iteration time can be reduced.

In the literature there is no apparent guide line to allocate the parameters for the BFO algorithm. In the proposed EBFO algorithm, we assigned the limitations for the algorithm parameters by considering the various stages of bacterium growth discussed in the book by El-Mansi and Bryce.

Stages of bacteria growth in a controlled environment are shown in below,

(i) Lag phase: Amendment of the cells to new environment take place and it is getting ready to begin reproduction.

(ii) Growth phase: In this stage with the help of chemo-taxis and swarming practice, the cells can reach the location of food source. The growth rate is proportional to the cell concentration and the nutrient quantity. When the cell reaches the sufficient food location, the growth rate is rapid. When the cell reaches the maximum growth, it begins reproduction.

(iii) Stationary phase: After growth and reproduction, the cell will reach a minimum biological space called stationary phase. Due to the lack of one or more nutrients, buildup of toxic materials and organic acids generated during the growth phase, cell growth is restricted.

(iv) Death phase: It is mainly due to the toxic by-products and depletion of nutrient supply. In this, a decrease in live cell concentration occurs. The cell with a minimum health is eliminated. The above process repeats until there exist a controlled environment such as constant temperature and pH.

In bacteria foraging algorithm, the total number of bacterium considered for the optimization practice plays a vital role in maintaining the optimization accuracy and algorithm convergence. The larger number of bacterium can offer an agreeable accuracy, but sometimes it may increase the computation time. In this paper, we performed a number of trials to fix the range of the bacteria group size. When the E. coli is placed in a controlled environment, it will reach the food source with the action of tumbling or swimming. The first half of the group swims towards the food and rest half of the group tumbles. The bacterium

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

which enters into the nutrient environment first, may grow earlier and starts the reproduction operation. Around 25% of cells may die due to lack of nutrients and build up toxic materials. The probability of bacterial elimination mainly depends on the bacteria at the noxious environment, initial population of the bacteria, and the bacterial with the reproduction process. The bacteria are living organism, which will act fast at toxic environment compared to the nutrient source. This process may help to fix the values for attract and repel signal strength.

4.4 Diffie-Hellman Key Exchange Algorithm

Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Although Diffie–Hellman key agreement itself is an anonymous (non-authenticated) key-agreement protocol, it provides the basis for a variety of authenticated protocols, and is used to provide perfect forward secrecy in Transport Layer Security's ephemeral modes (referred to as EDH or DHE depending on the cipher suite).

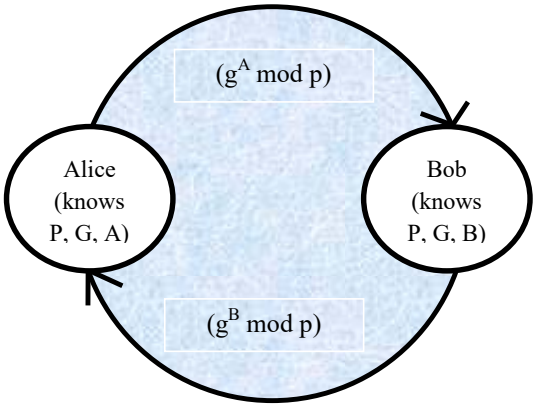

Figure 2: Diagrammatic representation of Diffie Hellman key exchange algorithm

Steps in the Algorithm:

Alice and Bob agree on a prime number q and a base g .

Alice chooses a secret number a , and sends Bob

$$A = g^a \bmod q \quad (5)$$

Bob chooses a secret number b , and sends Alice

$$B = g^b \bmod q \quad (6)$$

Alice computes

$$K_1 = B^a \bmod q \quad (7)$$

Bob computes

$$K_2 = A^b \bmod q \quad (8)$$

Both Alice and Bob can use this number as their key. Notice that q *and* g need not be protected.

An eavesdropper cannot discover this value even if she knows q *and* g and can obtain each of the messages. Hence by using this algorithm the nodes along with its messages are secured.

4.5 Elliptic Curve Cryptography (ECC)

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography (based on plain Galois fields) to provide equivalent security. The private and public keys are produced by the ECC method makes the encrypted data more safe. The general equation of the elliptic curve is given below,

$$y^2 = x^3 + ax + b \pmod q \quad (9)$$

Here a, b *and* q are random numbers and x ranges from 0 *to* $n-1$.

By substituting the above values we could get different values of y . Hence we could get different points. From these points we select private key. Public key is also calculated from private key. The formula for public key is indicated as follows,

$$pu(k) = pr(k) * q \quad (10)$$

Where,

$pu(k)$ *and* $pr(k)$ -indicates the public and private key.

Hence public key is calculated. Using these keys encryption and decryption is performed.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Encryption

Encryption is the process of converting information or data into a code, especially to prevent unauthorized access. Here two cipher text keys are generated and are as follows,

$$C1 = K * q \quad (11)$$

Where K ranges from $1 to n-1$

$$C2 = message + K * pu(k) \quad (12)$$

These are the two cipher text keys.

Decryption

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Using this method original message could be recovered.

$$Message = c2 - pr(k) * c1 \quad (13)$$

Hence the original message is recovered using the private key. Hence by using the public and private keys the messages are encrypted in the nodes. The encrypted messages are finally sent to the base station with the help of optimal cluster head.

5. RESULT AND DISCUSSION

This section gives a detailed view of the results that are obtained using our proposed Diffie Hellman key exchange and elliptic curve cryptography encryption methods. We have proposed the encryption and cluster formation algorithms for providing security to messages contained in the nodes. The proposed method is implemented in NS2. The experimental result and the performance of the proposed method are clearly explained in the following section.

5.1 Evaluation Metrics

By using the evaluation metrics end to end delay, Packet delivery ratio, throughput and packet loss, the performance of the recommended system is evaluated.

End-to-End Delay

End-to-end delay or one-way delay (OWD) refers to the time taken for a packet to be transmitted across a network from source to destination.

$$d_{end-end} = n[d_{trans} + d_{prop} + d_{proc} + d_{queue}] \quad (14)$$

Where,

$d_{end-end}$ = end-to-end delay

d_{trans} = transmission delay

d_{prop} = propagation delay

d_{proc} = processing delay

d_{queue} = Queuing delay

n = number of links (Number of routers - 1).

Packet delivery ratio

The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.

Packet drop

Some packets can also be lost because a router receives it and specifically decides not to pass it on to the next hop. This deliberate loss of a packet is called packet drop.

Energy

Energy is defined as the strength and vitality required for sustained physical activity. Energy consumption is defined as the communication overhead of the nodes where a certain number of false data are injected in to a network.

Overhead

It is defined as the average number of location claims that are sent and received by the nodes in the network.

Throughput

The throughput is the amount of data that can be sent from the sources to the destination.

5.2. Comparison Analysis

Comparison analysis of our proposed work is evaluated by varying the nodes 25, 50, 75, 100 and 125. Figures 3 to 8 show the delay, delivery ratio, drop, energy, overhead, and throughput. Thus our proposed work Optimal Key Management Technique for Secure Data Transmission OKMSDT has been compared with the existing work Key Management Data Transmission System (without optimization) KMDT.

Journal of Theoretical and Applied Information Technology
31st August 2017. Vol.95. No.16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

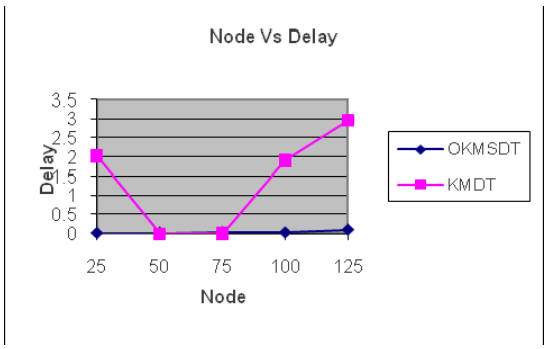

Figure 3: Comparison for Node vs. Delay

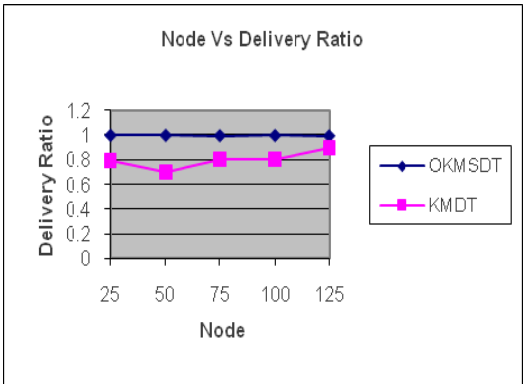

Figure 4: comparison for Nodes vs. Delivery Ratio

According to the experiment, the Figure 3 shows the delay performance of the proposed and existing method. During transmission, the proposed method decreases the delay and existing method delay increases with respect to the nodes. The Figure 4 depicts the delivery ratio of the proposed work OKMSDT and existing method KMDT. Delivery ratio of proposed method is higher than the delivery ratio of the existing method for varying nodes.

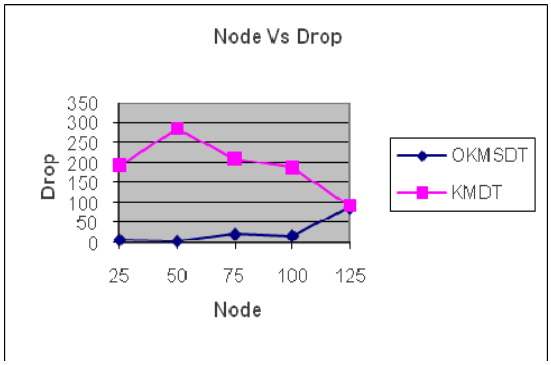

Figure 5: Comparison for Node vs. Drop

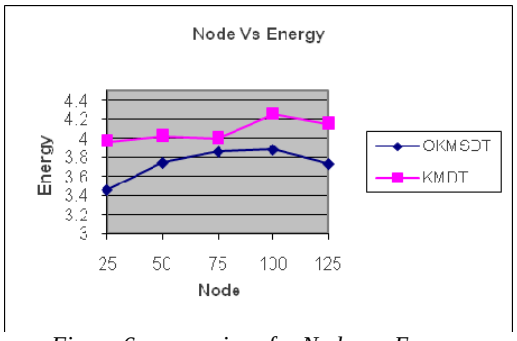

Figure 6: comparison for Nodes vs Energy

Drop comparison of the proposed method is shown in Figure 5 Drop decreases for the proposed method while the drop increases for the existing method. Figure 6 shows the energy comparison of the proposed and existing method. Energy consumption of the proposed method is less than that of the existing method. Overhead comparison of the proposed method and existing method is depicted in Figure 7. The Figure 8 shows the throughput comparison of the proposed and existing method. Throughput is high for the proposed method.

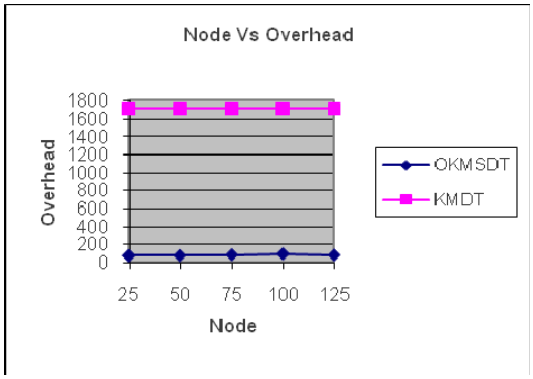

Figure 7: Comparison for Node vs. Overhead

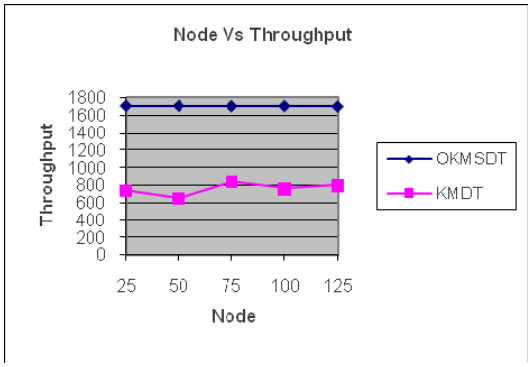

Figure 8: Comparison for Node vs. Throughput

Journal of Theoretical and Applied Information Technology
31st August 2017. Vol.95. No.16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Comparison analysis of our proposed work is evaluated by varying the nodal rate as 50, 100, 150, 200 and 250. Figure 9-14 shows the delay, delivery ratio, drop, energy, overhead, and throughput. Thus our proposed work OKMSDT has been compared with the existing work KMDT.

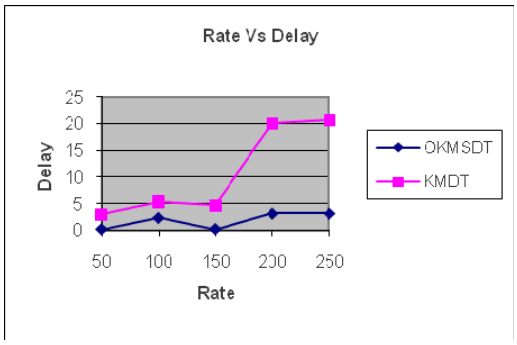

Figure 9: Comparison for Rate vs. Delay

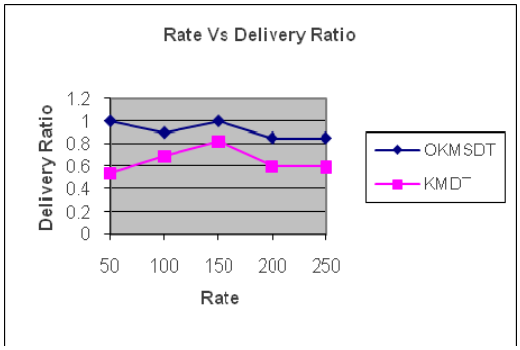

Figure 10: Comparison for Rate vs. Delivery Ratio

The Figure 9 represents the delay comparison of the proposed and existing method with respect to nodal rate. In existing method, the nodal rate goes high when the delay time increases but, OKMSDT shows less delay in high nodal rate. In Figure 10 indicates delivery ratio between proposed and existing method. The proposed method shows high delivery ratio compare to existing method.

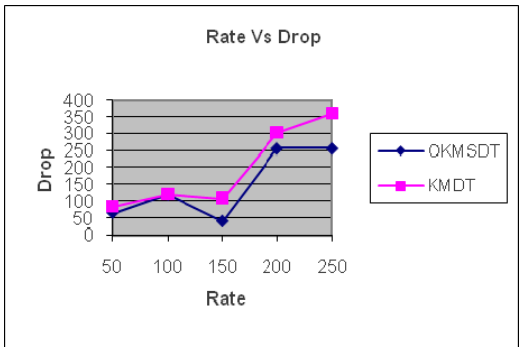

Figure 11: Comparison for Rate vs. Drop

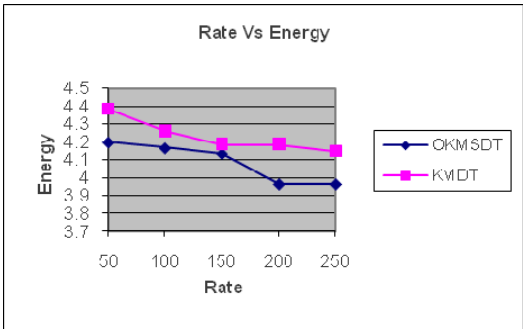

Figure 12: Comparison for Rate vs. Energy

Figure 11 shows the drop comparison of the proposed and existing method with respect to nodal rate. Compare to the existing method, our proposed method shows better result during transmission dropping data is less. Figure 12 represents the energy comparison between the existing KMDT method and proposed OKMSDT method. The OKMSDT method consumes less energy compare to the KMDT method.

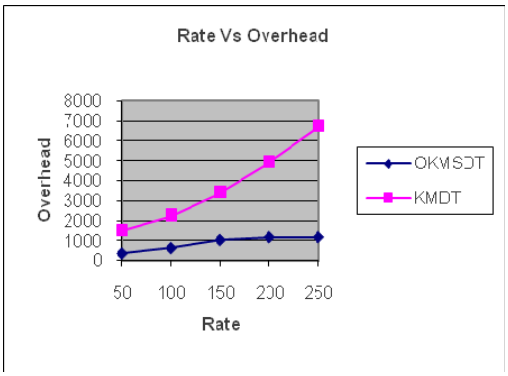

Figure 13: Comparison for Rate vs. Overhead

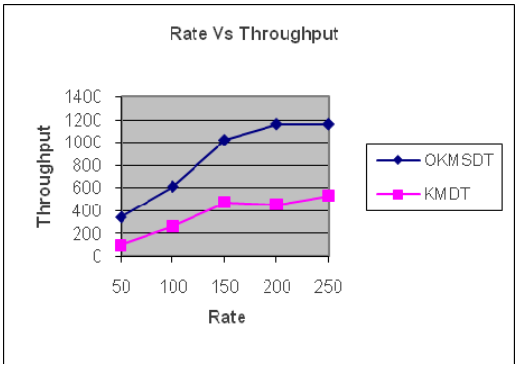

Figure 14: Comparison for Rate vs. Throughput

Figure 13 depicts the overhead comparison of the proposed and existing method. Overhead is low for the proposed method while it is high for the existing

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

method. Throughput comparison of the proposed method and the existing method is shown in Figure 14. Throughput rate is high for the proposed method.

6. CONCLUSION

Key management is vital part of security. Key management protocols play a key role in any secure group communication architecture. This study has confirmed that key management mechanism proposed to guarantee the security of conventional networks are not necessarily suitable or adaptable to MANETs. Novel techniques, designed specifically for MANETs, are necessary. Key management is an important area that will need resolution before wide-scale deployment of ad hoc networks will become practical. Although the key management for MANETs has reached a reasonable level of maturity, it is still a research area with room for innovation. When we have compared our proposed optimal key management secure data transmission system with the existing key management data transmission system, our proposed system has given better results and prove that our proposed system is better than an existing system. Further work will concentrate on refining the metrics. Additionally, it will be interesting to see whether the performance of the metrics may be enhanced by taking into account other factors such as signal strength. Finally, extending the link stability metric to a path rating metric seems promising for use in mobile ad hoc networks.

REFRENCES:

[1] M. Gerharz, C. de Waal, M. Frank and P. Martini, "Link Stability in MobileWireless Ad Hoc Networks", *Proceedings of 27th Annual IEEE Conference on Local Computer Networks*, 2002, pp. 30-39.

[2] H. Zhang and Y.N. Dong, "Mobility Prediction Model Based Link Stability Metric for Wireless Ad Hoc Networks", *Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing*, 2006, pp. 1-4.

[3] R. Zhang and J. Rubin, "Robust Flow Admission Control and Routing for Mobile Ad Hoc Networks", *Proceedings of IEEE Military Communications Conference*, 2006, pp. 1-7.

[4] S. Xu, K.L. Blackmore, and H.M. Jones, "An Analysis Framework forMobility Metrics in Mobile Ad Hoc Networks", *Journal on Wireless Communications and Networking*, Vol. 2007, No. 1, pp. 019249, 2006.

[5] S. Medidi, J. Ding, G. Garudapuram, J. Wang, and M. Medidi, "An analytical model and performance evaluation of transport protocols for wireless ad-hoc networks", *Proceedings of 41st Annual Simulation Symposium*, 2008, pp. 131-138.

[6] C. Curescu and S.N. Tehrani, "A Bidding Algorithm for Optimized Utility-Based Resource Allocation in Ad Hoc Networks", *IEEE Transactions on Mobile Computing*, Vol. 7, No. 12, 2008.

[7] E.R. Cavalcanti and M.A. Spohn, "Improved Spatial and Temporal Mobility Metrics for Mobile Ad Hoc Networks", *Proceedings of the Fourth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, 2010, pp. 189-195.

[8] N. Mehta, A.D. Hallen, and W. Wang, "Enabling Adaptive Rate and Relay Selection for 802.11 Mobile Ad Hoc Networks", *Proceedings of IEEE Wireless Communications Symposium*,2012, pp. 4150-4154.

[9] C. Curescu and S.N. Tehrani, "A Bidding Algorithm for Optimized Utility-Based Resource Allocation in Ad Hoc Networks", *IEEE Transactions On Mobile Computing*, Vol. 7, No. 12, pp.1397-1414, 2008.

[10] S. Leng, Y. Zhang, H.H. Chen, L. Zhang and K. Liu, "A Novel k-Hop Compound Metric Based Clustering Scheme for Ad Hoc Wireless Networks", *IEEE Transactions On Wireless Communications*, Vol. 8, No. 1, pp.367-375, 2009.

[11] S. Kumar, S.C. Sharma and B. Suman, "Classification and Evaluation of Mobility Metrics for Mobility Model Movement Patterns in Mobile Ad-Hoc Networks", *International journal on applications of graph theory in wireless ad hoc networks and sensor networks*, Vol.3, No.3, pp. 25, 2011.

[12] H. Zhang, Z. Zhang and H. Dai, "Gossip-Based Information Spreading in Mobile Networks", *IEEE Transactions On Wireless Communications*, Vol. 12, No. 11, pp.5918-5928, 2013.

[13] Y. Xia and C.K. Yeo, "Measuring Group Mobility: A Topology Based Approach", *IEEE Wireless Communications Letters*, Vol. 2, No.1, pp. 54-57, 2013.

[14] D.G. Reina, S.L. Toral, P. Jonhson and F. Barrero, "Hybrid Flooding Scheme for Mobile Ad Hoc Networks", *IEEE Communications Letters*, Vol. 17, No. 3, pp. 592-595, 2013.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[15] J.H. Cho and I.R. Chen, "Performance analysis of hierarchical group key management integrated with adaptive intrusion detection in mobile ad hoc networks", *Performance Evaluation*, Vol. 68, No. 1, pp. 58-75, 2011.

[16] D. Huang and D. Medhi, "A secure group key management scheme for hierarchical mobile ad hoc networks", *Ad Hoc Networks*, Vol. 6, No. 4, pp. 560-577, 2008.

[17] X. Zhao, F. Zhang and H. Tian, "Dynamic asymmetric group key agreement for ad hoc networks", *Ad Hoc Networks,* Vol. 9, No. 5, pp. 928–939, 2011.

[18] J.H. Choa, I.R. Chena and D.C. Wang, "Performance optimization of region-based group key management in mobile ad hoc networks", *Performance Evaluation*, Vol. 65, No. 5, pp. 319-344, 2008.

[19] Yanji Piao, JongUk Kima, Usman Tariq and Manpyo Honga, "Polynomial-based key management for secure intra-group and inter-group communication", Computers and Mathematics with Applications, Vol. 65, No. 9, pp. 1300-1309, 2013.

[20] J.C. Lin, K.H. Huang, F. Lai and H.C. Lee, "Secure and efficient group key management with shared key derivation", *Computer Standards & Interfaces,* Vol. 31, No. 1, pp. 192–208, 2009.

[21] S. Zhao, R. Kent, A. Aggarwal, "A key management and secure routing integrated framework for Mobile Ad-hoc Networks", *Ad Hoc Networks*, Vol. 11, No. 3, pp. 1046–1061, 2013.