I.J. Modern Education and Computer Science, **2014, 9, 28-35**
Published Online September 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2014.09.05

Sustaining Security in MANET: Biometric Stationed Authentication Protocol (BSAP) Inculcating Meta-Heuristic Genetic Algorithm

Sherin Zafar
Faculty of Engineering, Manav Rachna International University Faridabad, Haryana, 121004, India
Email:Sherin_zafar84@yahoo.com

Prof. (Dr) M K Soni
Faculty of Engineering, Manav Rachna International University Faridabad, Haryana, 121004, India
Email: ed.fet@mriu.edu.in

Abstract—The paper comprehends an impending accost of intensifying biometric stationed authentication protocol(BSAP) bestowing meta-heuristic genetic algorithm for securing MANET. Biometric authentication using fingerprint, facial, iris scan, voice recognition etc. have gain a lot of importance in recent years to provide security in MANET. Biometrics are more advantageous and secure as compared to prevailing data security techniques like password or token mechanisms. A higher level of security is achieved in our impending approach using genetic algorithm to overcome the security and privacy concerns that exist in biometric technology. The foremost requirement of our protocol is to overcome various data attacks such as wormhole, cache poisoning, invisible node attack etc. that are confronted by MANET and make the network more secure.

Index Terms—Biometrics, genetic algorithm, secure routing protocols in MANET, ICP.

I. Introduction Focusing On Pedagogy Of Impending Approach

In many whereabouts a communication network is vital where there is no rooted infrastructure and neither there is time to create such a framework such as military operations, law enforcement, rescue operations and personal area networking. A network developed in such situations where the nodes are mobile, are called mobile ad hoc networks (MANETs). An ad-hoc network is integrated robustly from scratch manipulating wireless connections and composed of mobile nodes. Mobile or motile ad-hoc networks will be used reciprocally in our paper which signifies similar meaning i.e. operative or adaptable ad-hoc networks. Content, pace of organization and less reliance on a permanent framework when grouped with conventional wireless networks are some of the unique features provided by MANET. Regardless, accessible distributed architecture, compelling network topology collated wireless mediocre, confined battery, memory and computation power like unparallel characteristics lead to various consequential demands on security parameters of MANET. Due to their dynamic nature a large number of specific confronts are faced by MANET as compared with the basic data networks .Due to the modification of various transmission properties specified by continuous movement of nodes a requirement of network initiation as well as maintenance occurs. Also a demand of repeated connectivity changes which includes regular entry and exit of various nodes, MANET must have the competence to acclimate and reflect the various topology transitions. All the nodes in ad-hoc networks have two aspects: originator and end-user in one stream of data packets, and routers for data packets doomed for the other nodes. The above demands lead to the advancement of various secure protocols for routing in MANET that aim to protect the network and hence enhance its performance. Currently there exist more than hundreds of routing protocols for MANETs. Defense mechanism of MANET against various types of attacks can be broadly categorized as: secure routing mechanism and security in packet transmission. Securing MANET can also be divided into proactive approach which restricts an attacker from instigating attacks, by applying various cryptographic mechanism and reactive approach that explores and exposes various threats and their countermeasures[1] . The prospective approach described in this paper is formulated under 5(five) main segments. Segment I, introduces ad-hoc network, and its various existing secure routing protocols, biometrics and meta-heuristic algorithm.Segment II, analyze the relevant analysis effort rendered towards security of MANET. Segment III, figures out the prospective work by asserting a new BSAP protocol. Segment IV, deals with simulation workflow. Segment V, comprises of conclusion and propositions leading to future analysis. The paper is concluded by acknowledgement and various references exploited in this paper along with details of the authors.

A. Current Secure protocols for routing in MANET

We focus on the prevailing secure routing protocols in

Copyright © 2014 MECS

MANET and how their discrepancies can be avoided by our impending genetic based biometric stationed authentication protocol for MANET.

►***Ariadne:*** DSR prevents removing any current nodes or adding additional nodes along the network route by any intermediate node A secure addendum to provide security in DSR is Ariadne [2].Prevention of "wormhole attack"(establishing a continuous wormhole link between two points in the network and eavesdropping various intruded messages through the network) and cache poisoning attack(attacker conveniently affect the libertine mode of updating a routing table , where a node updates its own cache on snooping a packet even if it is not on the path of that node) is not possible in Ariadne which leads to security breaches, also it suffers from complicated key exchange mechanism[2].

►***SAODV:*** Protocol developed to provide security to AODV. SAODV substantiate non-erratic fields of route request packet (RREQP) and route reply packet (RREPP) by employing digital signature which exploit one-way mutange (hash) string (chains) to substantiate the hop tally (counts). Here, two malignant nodes affirm a link amidst them, and allow traffic through them. Public key cryptography compels eminent processing sustenance.

►***SAR:*** It employs a routing approach that amalgamate various security stages of nodes into prescribed routing metrics. SAR provides nothing regarding applying security stage as a metric and since no proper security approval is available, route discovery system may abort, in spite of connectivity path between the relevant destination.

►***SEAD:*** A proactive secure protocol for routing in MANET stationed on DSDV-SQ-protocol. SEAD uses one-way melange (hash) chain for protection rather than traditional asymmetric encryption, which are engrossed quickly hence these chains should be either longer or librated regularly.

►***SDSDV:*** In SDSDV if no two nodes are in an association, a node propitiously recognizes a malignant routing amend (update) accompanying any sequence number or distance artifice, and exploits cryptographic technique for substantiation [3].SDSDV results in large network sustenance (overhead).

►***SLSP-*** It secures the identification and allotment of a link state information by appointing each node with a public/private key pair. SLSP is quite susceptible to intriguing attackers.

►***SRP***: It establishes a security union (association) amidst the source(S) and the destination (D) node. SRP reveals network anatomy with un-encrypted routing path and affected by "invisible node attack"(any node that adequately cooperates without exposing its identity is an invisible node and the attack called as invisible node attack) [3].

►***ARAN:*** It employs public key cryptography hence all nodes apperceive the actual next hop along a route from source(S) to destination (D). Consequence of above cryptography process is that ARAN faces number of issues regarding extra memory and large processing sustenance for encryption. Whether the perceived path is exemplary (optimal) is not guaranteed since ARAN doesn't avail hop count.[4].

Hence, discussing the various disadvantages that occur in the existing secure protocols of ad-hoc networks, we propose a biometric stationed authentication protocol (BSAP) using meta-heuristic genetic algorithm which will embed the features of biometric technique, genetic algorithm and cryptography hence leading to a three level protection thus rendering more security to ad-hoc networks.

B. Necessity of Biometrics Security

Security requirements are quite demanding for mission-captious applications such as a military, access control and monitoring therefore secure protocol developed for ad-hoc network must combine both biometrics and cryptography techniques embedded with genetic algorithm to make the system more secure. Biometrics, clearly is the evaluation and employment of the exclusive features of humans beings to categorize from each other. Biometrics exemplify the approaches for exclusively diagnosing human behavioural traits which fall under the categories of strong biometrics that acquire high distinctive content and great extent of stability, like fingerprints, DNA, iris, retina, etc , whereas weak biometrics possess low distinctive content and changes gradually, like hand-geometry, face, keystroke dynamics, etc. The indulgence amid the various biometric technologies brandish on the application and security . The strong biometric technologies that can readily be adaptable in MANET are fingerprints and iris recognition. From many years fingerprints and iris have been propitiously used in human identification due to their resolute and unique nature throughout human life. Biometrics are conferred as congenital identification tool that cannot be acquired, stolen, or jilted, and duplication is impractical hence provide greater security and authentication in MANET. Although biometric provide number of advantages some security and privacy apprehensions still can occur:

►Biometric can be genuine but not necessarily private (secret).
►Eliminating or abolishing biometric is not possible.
►If once lost, biometric are exposed permanently.
►To apprehend humans, cross-matching is employed barring their approval.

Consequently impinging the constraints of biometrics as discussed, some features of original biometric are taken and transposed using meta-heuristic based genetic. algorithm. If anyhow arbitration of biometric takes place, retraction is done by adopting different property set and distinct genetic procedure, hence conserving continuity and confidentiality of the biometric.

C. Meta-heuristic Algorithm

Meta-heuristic algorithm is an illustrious method consummated to credit, commence or stipulate a lower-level scenario or heuristic (partial exploration algorithm)

that execute a relevantly admissible definition to optimization dilemma, confined with remarkable compressed intelligence or cramped data processing capability. They are pertinent for various complications that make deficient hypothesis about the optimization problem being elucidated. Categorization of meta-heuristic algorithms is specified as (based upon their various properties):

- ►Genetic algorithms (GA)
- ►Neural Network (NN) with Artificial Intelligence (AI)
- ►Simulated (Artificial) annealing (SA)
- ►Tabu-search or Tabu- exploration (TS or TE)
- ►Ant colony optimization (ACO)
- ►Evolutionary computation or Evolutionary estimation (EC or EE)

D. Genetic Algorithms (GA's)

Genetic algorithms [5] are algorithms under the category of estimating illustration determined through intrinsic transformation. These algorithms are accustomed by three imperative operators:

►**Selection:** This operator accomplishes its task by choosing the competent (fittest) distinctive chromosomes, designated as parents chromosomes that augment population of chromosome generation.

►**Cross-over:** This operator uses competent parent chromosomes of selection operator as its input and commix them to figure out child chromosomes for successive subsequent propagation.

►**Mutation:** Preserving genetic diversification of a population generation of individual chromosomes to next generation by altering from their original state their one/more gene values is done by mutation operator. Mutation takes place concurrently with evolution conceding a user -defined probability which should be kept as low as possible because keeping it high can lead to a primeval random exploration. This operator may cause genetic algorithm resulting in a preferred elucidation (solution) since here the elucidation may alter completely from the former. Mutation is applied basically if the algorithm gets stuck in condition referred as local minima, thus impeding chromosome population by adapting identical characteristics of each other resulting in reduced speed or even deterred evolution. Therefore it is referred in our paper that mutate if necessary.

II. Relevant Analysis

Relevant Analysis deals with succinctly demonstrating various explorations carried out for securing MANET including the numerous advances of biometric security, cryptography as well as exploring use of genetic algorithms .

Ananda Krishna.B et al. [2] have characterized a model based on collective algorithms for encryption and decryption which is done by employing one of the algorithms selected in a random manner hence its difficult to apprehend either algorithms or keys. For profound traffic network with great mobility, the model performs better.

Anand Patwardhan et al. [6] advanced proposition of protocol which leads to secure routing and established using AODV structure over IPv6.Intrusion Detection is reinforced by a response system for ad-hoc networks.

Zarza L et al. [7] have exemplified consideration of Genetic Algorithms as an assisting medium to conclude security protocols, hence leading to optimized elucidation for MANET. The paper optimizes problems by exploring security protocols refined for MANET as binary strings and applying genetic algorithm to genome assimilation.

Abhishek Roy and Sajal K Das. [8] have envisaged a protocol to attain QOS by generating near-optimal routes in MANET. The protocol conceives QOS designated instantaneous-best routes that pursue multicasting and avoid repetitions, even with rudimentary network knowledge which is specified by simulation results.

Rajaram.A and S.Palaniswami[9] have accomplished trust in MANET through a secure protocol which employs cross-layer approach aiming towards confidentiality and authentication of packets in distinct layers.

Qinghan Xiao [10] has led to the development of a new approach for authentication by maintaining the biometric figures of all group participants. Distributed instead of a central authentication is employed. High security is provided through mutual cryptographic key applied for articulation inside a limited alliance and not suited for large enterprise management.

Jie Liu et al. [11] advised an optimum biometric-stationed constant substantiation (authentication) design for MANET which characterize through: user-to-device and device-to-network. The approach targets the user-to-device branch and optimally administer to accomplish authentication and employ biometrics to reduce the utilisation of network resources.

Shanthini.B et al. [12] have developed Cancellable Biometric-Based Security System (CBBSS) where biometrics cancellable in nature is employed for securing information in MANET. Fingerprint constituent of receiver are coupled with the tokenized melange data by applying an algorithm referred as inner-product. The result of this algorithm is stationed on a threshold value to develop a set of independent (private) binary cipher referred as cryptographic key in the system.

Copyright © 2014 MECS

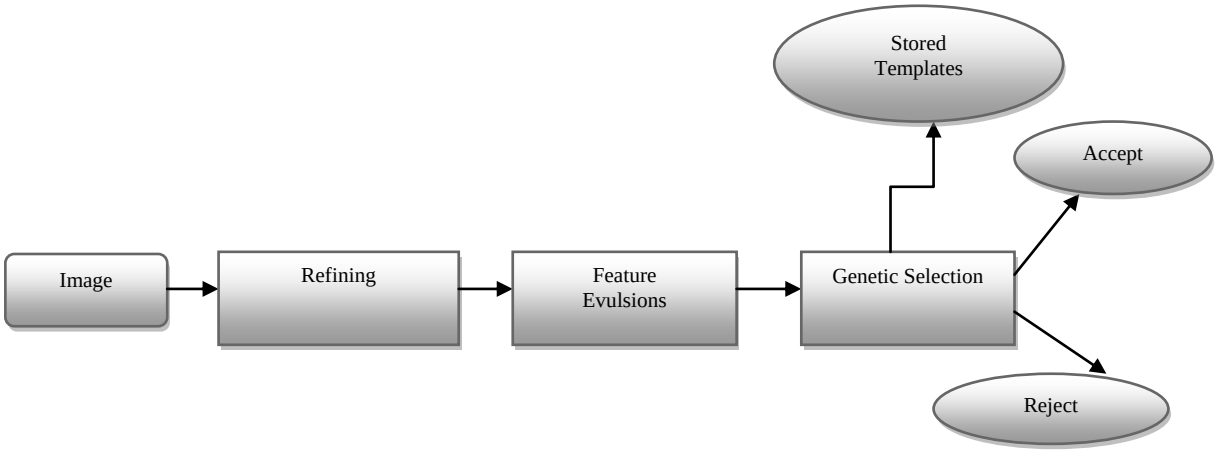

Fig.1.ICP Process

III. Prospective Work

In the recommended biometric stationed authentication protocol (BSAP) bestowing meta-heuristic genetic algorithm, one of the operator of genetic algorithm referred as crossover which is further characterized as 2-bit or Modifying(Adaptive) is enforced on biometric characteristic set to overcome its constrains hence enhancing security of MANET. The prospective approach focuses in overcoming the limitations of previous secure routing protocols by combining features of biometrics, GA and cryptography hence providing authentication and thus enhancing network performance

A. Procreation of Genetic-Stationed Biometric Key by employing Iris Connotation Process(ICP)

In our prospective protocol every node in MANET cultivate biometric impressions of each and every other node. BSAP can exploit both fingerprint and iris specifications but in this paper we will exploit strong biometric i.e. iris. If a source node transfers a message to any destined node, the source undergoes an iris connotation process (ICP) which starts with procurement of eye. Images are refined to align the scale and radiation of the iris and localize the iris pattern .Then follows feature evulsions which selects the fittest 'q' chromosomes for crossover. Selected chromosomes undergo 2-bit/ Modified (Adaptive) crossover operation of genetic algorithm since it has the competence to arouse, adopt, and constitute blocks for modeling individual optimum strings. If required, percolate the last operation of genetic algorithm, namely mutation with probability 0.01 which results in generating cryptographic key by employing either Fiestel or DES key generation algorithm for the protocol which is depicted in Fig.2. Receiver exploits his biometric to institute the corresponding cryptographic key and the similar genetic operations are employed for decryption as well. A new key is generated by applying the above mentioned procedure if the generated biometric stationed key is implicated.

B. Proposed algorithm for BSAP inculcating GA:

The proposed algorithm for developing BSAP inculcating GA is described below:

1. If a source node transfers a message to any destined node, the source undergoes an iris connotation process(ICP) shown in Fig.1 which starts with procurement of eye.

2. ICP(Iris Connotation Process)

***Refining**

The attained image perpetually contains not only the effective component (IRIS) but may also include some components like eyelid, pupil & reflection which are not propitious for our work. Circumstances like the illumination not regularly scattered, distinct eye-to camera purview may conclude distinct image dimensions regarding same eye.So refining undergoes a iris dissolution process which exploits Daugman's integro-differential operator for ascertaining iris as well as pupil contour [26] which is illustrated by the given equation:

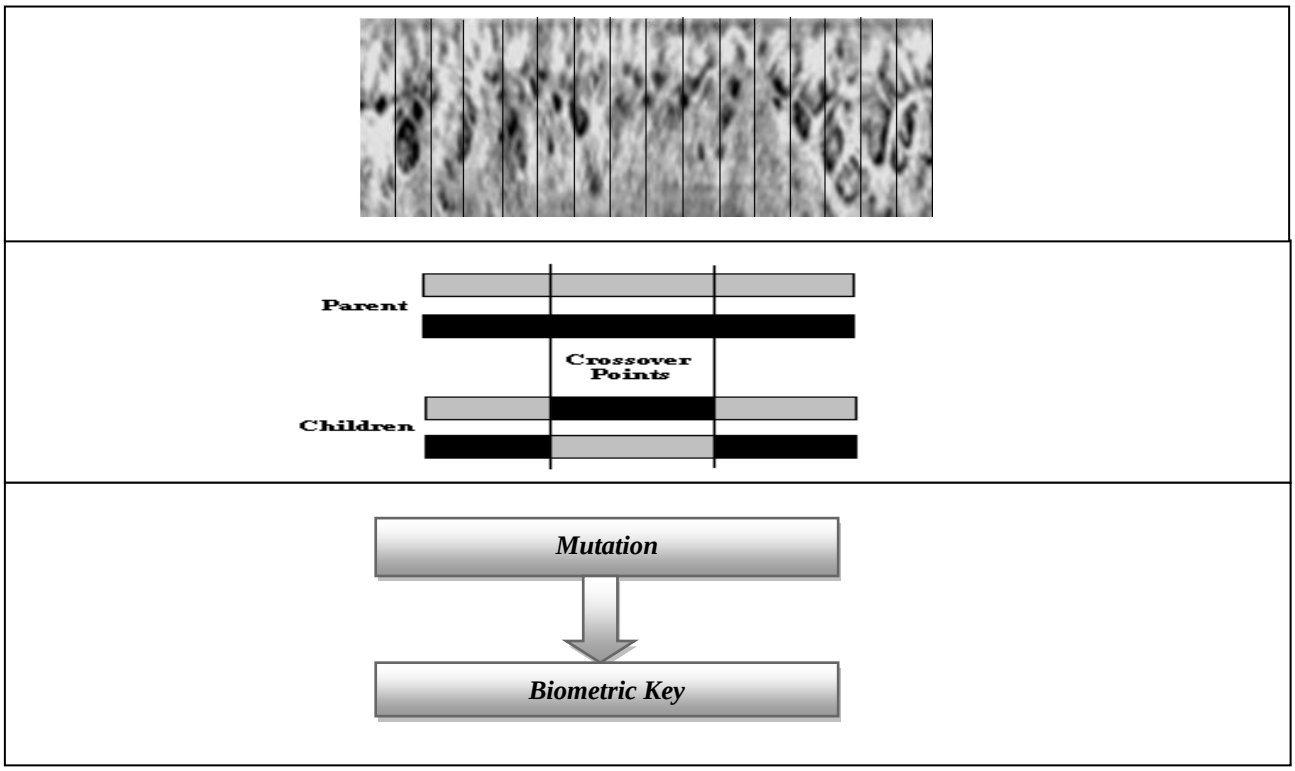

Fig.2. Generation of biometric key from refined iris

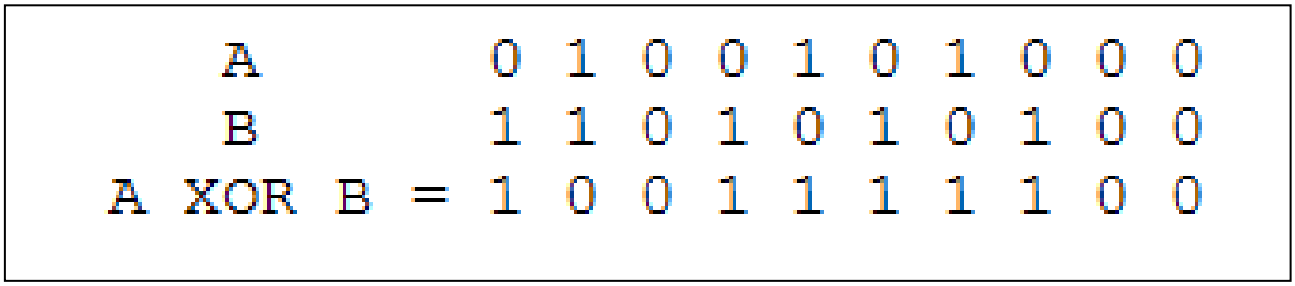

Fig.3.Generation of Hamming Code

$$Max(r, x0, y0)G\sigma(r) * \partial \div \partial x \int r, x0, y0I(x, y) \div 2 \prod rds - -(1)$$

where:

- ►r, x0, y0: This is specified as the centre and radius of coarse circle (it is referred for each pupil as well as iris).
- ►Gσ (r): This is the Gaussian function.
- ►∂r: This is the radius extent (range) utilised to penetrate I(x, y) of the initial iris image.

Iris localized structure is altered through Daugman's dissolution algorithm from Cartesian to polar coordinates. Intensification of the image is carried out by Histogram Equalization method.

***Feature Evulsions**

Feature evulsions is the most important process which includes Iris Cipher Propagation for converting a two dimensional image into arithmetic framework. Fig. 2.shows dissolution of iris image into primary cell range for propagation of iris cipher. Pixels undergo standard deviation which is exploited as an exemplary value of a primary cell region for estimation. We evolve 16 bit values which need to be transformed, contemplating the boundary value as mean against all blocks. Make pixel value 1 if the original value is larger than boundary value otherwise a 0.e.g. Iris Code: 1 0 1 0 0 1 0 0 0 1 1 1 1 1 1 1

Copyright © 2014 MECS

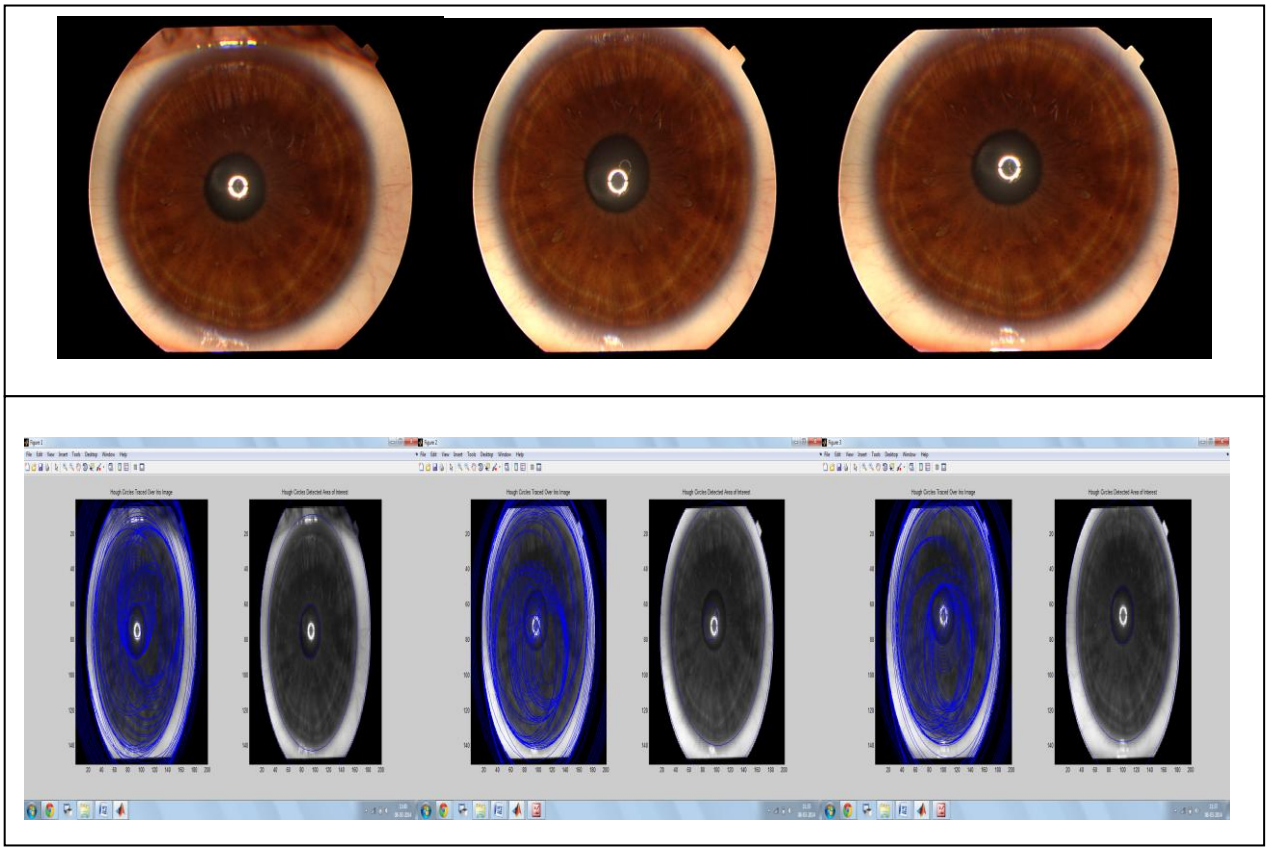

Fig.4. Results Images Showing the ICP Process

Next generating the hamming length(distance) amidst two bit templates to draw a conclusion whether the two templates were from distinct or same irises. Hamming length amidst two strings is the analogous bit positions difference between them.

In Fig.3. the hamming code amidst the above 10-bit strings is 6 i.e. the number of 1's in the XOR string .The iris is correlated to earlier accumulated iris code to enumerate the hamming distance amidst them. Number of bits difference between two iris code is the hamming distance between them. Hence the hamming distance of an iris code to itself is 0, to its complement is 1 and (expected distance) between 2 random iris codes is 0.5.

3. Accomplish crossover operation of genetic algorithm by executing 2-bit or Modifying (Adaptive) crossover techniques

4. Carry out mutation operation with probability 0.01 if required.

5. Thus by applying the above mentioned operations a cryptographic key is produced by employing either DES Fiestel network or AES key generation.

6. Relinquish the above mentioned steps until optimization is achieved.

C. Ensuring Security of Data in MANET

Ensuring security of data through BSAP is done by applying the above developed key to encrypt the original message using a simple cryptographic algorithm. DES fiestel network or AES algorithm can be exploited. Here we will be discussing about AES method where encryption as well as decryption operations are stated by the formulae:

Cipher-text = Encryption Algorithm BGK (Plaintext)
Plaintext = Decryption Algorithm BGK (Cipher-text)

where:

BGK - Biometric Genetic Key (created by Recipient Biometric)

Advanced Encryption Standard(AES) is a type of non-Feistel cipher in which 10, 12, or 14 rounds are employed to encrypt as well as decrypt a data block of 128 bits in size. Key size which is contingent upon on the number of rounds can be 128, 192, or 256 bits. Various terminologies that are specified in AES are:

►**In Matrix:** It is single 128 bit block(input of algorithm) utilised both for decryption as well as encryption

►**State Array:** It is a reproduction of in matrix which is altered at each level and hence reproduced as an output matrix.

►**W Matrix:** It is the elaboration of the key into an array of key schedule words.

►**Add round key:** This level records the starting of the algorithm subsequently by 9 rounds of four stages and a tenth round of three stages ,applying both for encryption as well as decryption.

The four levels of the algorithm are specified as substitute byte, shift rows, mix columns and add round key. The tenth round directly leaves out the **mix columns** level. The starting nine rounds of the decryption algorithm consist of inverse shift rows, inverse substitute bytes, inverse add round key and inverse mix columns. Repeatedly, the tenth round directly leaves out the **inverse mix columns** level.

D. Features accomplished by our proposed protocol:

►**Confidentiality**: The protocol helps in maintaining the privacy of the data. Consider the situation where the attacker tries to acquire the primitive directive(message) against the text which is encrypted, leads to the requirement of cryptographic key. The developed key can be acquired only through recipient biometric. Additionally the biometric is not used in its original form rather a cancellable interpretation is exploited that makes computationally inconceivable to acquire the key.

►**Authentication:** Through the proposed BSAP, the participants of MANET corroborate every participant through their respective biometric. At the time of receiver verification of the message to check whether or not it is through a valid sender, the message is encrypted by acquiring the sender's biometric and the receiver explores the same biometric to decrypt the message.

►**Lightweight:** It considerably extends network lifetime, by specifying the application of ciphers which are computationally efficient like the symmetric-key algorithms and cryptographic hash functions.

►**Integrity:** Integrity is maintained in BSAP through the recipient verification to check whether the received message is the actual message transmitted by the sender. If the intruder by any chance tries to change the cipher-text, the authentic plaintext will not be developed after trying to decrypt through the key created by employing recipient biometric.

►**Cooperative:** It accomplishes high-level security with the aid of mutual collaboration amidst various nodes along with other protocols.

►**Attack-tolerant:** This property will facilitate the network to resist various attacks.

►**Flexible:** Flexibility maintains security for energy consumption.

►C**ompatibility:** The protocol is compatible with the various security methodologies and services in existence.

►**Scalability:** The protocol is scalable to the rapidly growing network size.

IV. Simulation Workflow

Figure 4. shows the implementation of ICP process that will be employed in the BSAP protocol. As discussed before the attained image perpetually contains not only the effective component (IRIS) but may also include some components like eyelid, pupil & reflection which are not propitious for our work. Circumstances like the illumination not regularly scattered, distinct eye-to-camera purview may conclude distinct image dimensions regarding same eye.

So the 3 sample iris images in figure 4. depict the how application of the iris connotation process on these images help us to retrieve the best parts of the iris section that result in proper biometric matching and thus secure ad-hoc networks. The experiments are performed through MATLAB platform.

V. Conclusion And Future Work

The paper, focuses on sustaining security and in MANET through biometric stationed authentication protocol (BSAP) inculcating meta-heuristic genetic algorithm**.**First phase of the protocol generates strong biometric features which can be fingerprint or iris, but here in this paper we have taken iris which undergoes an iris connotation process and hence generates fittest offspring which then undergo various genetic operations to overcome the shortcomings of biometrics. A biometric cryptographic key is produced to enhance security of MANET. Hence data is protected by applying three levels of security by our prospective approach which develops trust between various nodes of ad-hoc network.

Future enhancement includes simulating the proposed scheme through a network simulator and comparing it with the previous secure protocols like SEAD, SAR, SRP etc .We will evaluate mainly the performance according to the following metrics.

►**Control overhead:** It specifies as the total number of routing control packets normalized by the total number of received data packets.

►**Average end-to-end delay:** It's the average of all surviving data packets from the sources to the destinations.

►**Average Packet Delivery Ratio:** It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

The simulation and comparison results will be presented in the next paper.

Acknowledgment

The authors wish to thank Professor Sufiyan Beg, Professor Department of Computer Engineering, Aligarh Muslim University, for his support and guidance throughout this paper.

References

[1] Hao.Y et al., "Security in Mobile Ad-hoc Networks: Challenges and Solutions", IEEE *Wireless Communications,* 2004.

[2] Ananda Krishna.B, Radha.S and K Chenna Kesava Reddy, "Data Security in Ad hoc Networks using Randomization of Cryptographic Algorithms*", Journal of Applied Sciences, pp. 4007-4012*, 2007.

[3] Tao Wan,Evanglelos Kranakis, P.C. van Oorschot, "Securing the Destination Sequenced Distanve Vector Routing Protocol".

[4] Hahill.B et al., "Secure Protocol for Ad-hoc Networks",*OEEE CNP*,2002.

[5] Fessi B A, Ben Abdullah, S.Hamdi Mand Boudriga, "A new genetic algorithm approach for intrusion response system in computer networks", IEEE *Symposium on Computers and Communications, pp. 342-347,* 2009.

[6] Anand Patwardan, Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis "Secure Routing and Intrusion Detection in Ad-hoc Networks" *Third* IEEE *International Conference on Pervasive computing and Communications, March* 2005.

[7] Zarza L., Pegueroles J and Soriano M "Interpretation of Binary Strings as Security Protocols for their Evolution by means of Genetic Algorithms.

[8] Abhishek Roy, Sajal K. Das, "QM2RP: A QoS-Based Mobile Multicast Routing Protocol Using Multi-Objective Genetic Algorithm", *Center for Research in Wireless Mobility and Networking (CReWMaN),* 2004.

[9] Rajaram.A,S.Palaniswami"A Trust Based Cross Layer Security Protocol for Mobile Ad hoc Networks", *(IJCSIS) International Journal of Computer Science and Information Security, pp.Vol. 6, No. 1,* 2007.

[10] Qinghan Xiao, *"A Biometric Authentication Approach for High Security Ad hoc Networks", Proceedings of* IEEE *Workshop on Information Assistance, pp. 250-256,* 2004.

[11] Jie Liu, F. Richard Yu, Chung-Horng Lung and Helen Tang, "Optimal Biometric-Based Continuous Authentication in Mobile Ad hoc Networks", *Third* IEEE *International Conference on Wireless and Mobile Computing, Networking and Communications, pp. 76-81,* 2007.

[12] Shanthini.B and S. Swamynathan "A Cancelable Biometric-Based Security System for Mobile Ad Hoc Networks", *International Conference on Computer Technology (ICONCT 09), pp. 179-184,* 2009.

Author's Profile

Sherin Zafar is an B.E ,M.Tech in Computer Science and Engineering from RGPV Bhopal in 2006 and 2010 respectively. Sherin is pursuing her PhD degree in Computer Engineering from Manav Rachna International University Faridabad 2011-12 batch. She is now Assistant Professor in Computer Section in Faculty of Engg. Jamia Milia Islamia New Delhi. In teaching, she has been focusing on Computer networks, DBMS etc. Her research interests include ad-hoc networks, meta-heuristic algorithms and network security.

DR. M.K Soni has degrees of BSc Engg , MSc Engg and PhD with 40 years of academic experience. He is currently Executive Director and Dean in Faculty of Engineering Manav Rachna International University Faridabad. He was formerly Professor in NIT Kurukshetra. His current research areas include microprocessors and microcontrollers.