ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (303-314), Month: October - December 2015, Available at: www.researchpublish.com

Security in MANET Routing Table from DOS Attack Using Cryptography Model

Parameswaran T.[1], Dr. PalaniSamy C[2], Elankathir.E[3]

Teaching Fellow, Department of CSE, Anna University Regional Centre, Coimbatore, India[1]
Professor and Head Of The Department of IT, Bannari Amman Institute of Technology,Erode[2]
PG Scholar, Department of CSE, Anna University Regional Centre, Coimbatore, India[3]

Abstract: **A mobile ad hoc network (MANET) is number of mobile nodes forming a temporary network. The mobile nodes are connected by wireless links to form a dynamic topology creation. The nodes are free to move randomly. As nodes travel often, it won't be having an unchanging infrastructure as a result it is unsafe and will be inclined by various attacks. Each node has a finite interaction range, which will be behaves as a router to communicate the packets to another node. The main problem in MANET is that, the routing tables which consists of each neighbour node information which maintained by the each node for the dynamic topology creation which is insecure. So to overcome this drawback, an optimized FMNK (Finger print Minutiae point non-invertible Key) algorithm is produced utilizing Biometric image models are introduced which can afford security and authentication. An optimized FMNK-AES-256(Finger print non invertible key Advance Encryption Standard) encryption algorithm is being introduced to encrypt the information applying a key to increase the security in MANET. In MANETs, performance may decrease when the networks size is beyond a certain threshold. As a result, when the network's size is small, many routing algorithms perform well. A clustering structure improves the network's scalability and fault tolerance, and reduction of communication overheads.**

Keywords: **MANET, FMNK, Biometrics, Fingerprint Minutiae, Inter/Intra cluster Routing, CBR, Authentication, Security.**

I. INTRODUCTION

A Mobile Ad hoc Network is a mobile nodes associated by wireless links which creates a network in the form of a dynamic communication graph for a wireless network. There won't be any stable infrastructure in MANET as a outcome the network topology is dynamic, as shown in Fig 1. This feature makes vulnerable to security attack. As nodes travel often, it won't be having an unchanging infrastructure as a result it is unsafe and will be inclined by various attacks. An intruder tries to create false messages among two nodes or group of nodes in process to trouble the network operation which is called the Denial of Service (DOS) attack. In computing, a denial-of-service attack is an attempt to make a machine, network resource unavailable to its users or indefinitely interrupt or suspend services of a host connected to the Internet. In wormhole attack, when the message is passed from starting node to end, a destructive node takes the packets from starting node fleeting the data to another destructive node through a route known as tunnel.

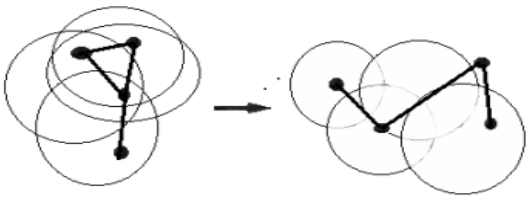

Fig 1: Mobile Adhoc Network

An optimized FMNK (Finger print Minutiae point non-invertible Key) algorithm is produced utilizing Biometric image models are introduced which can afford security and authentication. Biometric image models are introduced which can afford security and authentication. Biometrics is related to human characteristics. Biometrics is used in an authentication to form identification, verification, access control. It is used to identify individuals in groups. An optimized FMNK-AES 256 (Finger print non invertible key Advanced Encryption Standard) encryption algorithm is being introduced to encrypt the information applying a key to increase the security in MANET. AES algorithm provides highest security levels compared to the other encryption algorithm because of its large key size.

II. RELATED WORK

Biometrics- Based Cryptographic Key Generation:

As an alternative using PINs and passwords of cryptographic keys that are either simple for fail to remember or susceptible to dictionary attacks, and difficult-to-transfer keys can be created to the biometric information. It creates stable cryptographic keys from biometric image model data that is unbalanced in nature. The user-dependent transforms are used to create more condensed characteristics. Thus, a longer and steadier bit stream can be created as the cryptographic key. The evaluation can be carried verification and validation of fingerprint images. The output are obtained is highly cheering.

An Efficient Approach on Non-Invertible Cryptographic Key Generation from Cancellable Fingerprint Biometrics:

The main disadvantage of the cryptographic algorithms is the preservation of their keys secrecy. In the users biometric generation are strong and repeatable cryptographic key has gained from huge popularity. The randomness of the user biometric feature, incorporated into the generated cryptographic key, make the keys in order that it cannot be cracked by the attacker lacking worthy information of the user biometric. A person biometric is missed once; it will be helpful for the attackers as it is belonging to the user. To deal with this problem, cancellable biometrics can be used as a more effective answer for cancelling and reproducing biometric templates. It is to create a non-invertible cryptographic key from cancellable fingerprint minutiae point templates. In the beginning, one way transformations are applied on the minutiae point from the fingerprints, to accomplish a set of transformed points. Accordingly, the transformed points are most use to produce cancellable templates. The cancellable fingerprint templates are mostly used to create a unique non-invertible key.

Cancellable Finger Print Templates:

To create cancellable finger print templates with verification security based on the fingerprint verification. In a user can be many biometric identifiers as required by produce a new transformation key. The identifiers can be cancel and replace when cracked by attackers. The performance of several algorithms are used, surface folding transformations, polar, and Cartesian, of the minutiae positions are compared.

Fingerprint Biometrics Security:

A fingerprint biometrics securely stored the data does not adequate to rebuild the initial fingerprint biometric. A database security does not result in loss of biometric information. The stored information is more adequate to validate a search fingerprint. It is according to the utilizing of distributed source code methods are implemented with graph based codes. It provides a statistical model of the relationship among the biometric and the noisy biometric measurement considering in the process of authentication and security. It can be provides the ways to accept or refuse a candidate biometric probe and it provided the query with the stored encoded information. The effectiveness tested on a database containing more data sets, all consists approximately measurements of a single finger.

One Way Transformation:

It is how to measure the success of a particular transformation and matching fingerprints minutiae points. The key dependent geometric transform that is applied to the features extracted from a fingerprint, to generate a key dependent cancellable template for the fingerprint. It also investigates the performance of an authentication and security system that use this cancellable fingerprint. when a fingerprint matching algorithm is used for detection in accurate fingerprint image. It protect face biometric data using one way transformation in which original face images cannot be retrieved. The secure and reusable templates are generated by utilizing the transformed signatures of the face biometric and a multi space random projection. Using authentication is conducted on the transformed templates.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (303-314), Month: October - December 2015, Available at: www.researchpublish.com

Weighted Clustering Algorithm:

The weighted distributed clustering algorithm takes into battery power of mobile nodes, mobility, and broadcast power. Each node in the cluster requires the weight values of all other nodes and gathers the information of other cluster heads. The region the node travels and it is not enclosed in any cluster head, for this the system call upon the cluster set up procedure.

Cluster Based Routing Algorithm:

In MANETS, the Clustering Based Routing approach provides a solution for decrease routing control overhead and improves the network scalability. The group a node into clusters in each cluster one node acts as a cluster heads in order to reduce communication and control overheads. The major Design of Cluster Based Approach is to minimize on-demand route discovery traffic and use local repair to reduce route acquisition delay and new route discovery traffic.

FINGER PRINT MINUTIAE POINT NON-INVERTIBLE KEY:

a) Biometrics:

The biometric for use in a specific application involves a weighting of several factors like universality, acceptability, permanence, measurability, uniqueness, and performance. Universality means that every person using the system must process the particular image. Uniqueness means that the biometric should be sufficiently different from one person to another so that they can be distinguished in MANET. Measurability means the ease of acquisition and matching of the particular bio hash. Permanence is the variation of the biometric with time. It will be almost invariant with respect to take time. Acceptability means the adoption of the technology by the general population. Measurability means the ease of acquisition and matching of the particular bio hash. Performance is related to speed, efficiency and robustness of the technology used. A biometric system can be operated in two processes. There are verification and identification. In verification performs a one to one comparison of a captured biometric with a template stored in a biometric database in order to verify that individual is the person.

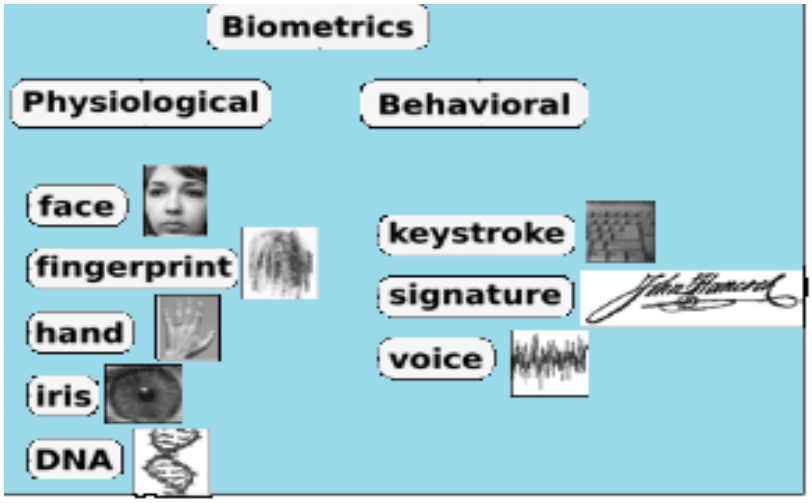

Fig 2: Different classes of biometrics

In identification performs a one to many comparison of a biometric database in an attempt to establish the identity of the unknown individual. Verification can only be used for positive recognition whereas identification can be used for both positive and negative recognition. It will succeed in identifying the individual if the comparison of a biometric sample to a template in the database within a previously set threshold. An individual uses the biometric system for the first time, the process is called enrolment. This process during the biometric data of the individual is recorded and stored.

b) Fingerprint:

A fingerprint is an impression left by the friction ridges of a human finger. In wider use of fingerprint image are the traces of an impression from the friction ridges. Impressions of fingerprints may be left on a surface by the secretions of the friction ridge skin, or they can be made by substances transferred from the peaks of friction ridges on the skin to a smooth surface.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (303-314), Month: October - December 2015, Available at: www.researchpublish.com

c) Minutiae Extraction:

A fingerprint is containing the pattern of ridges and valleys. In each individual has a unique fingerprint. The uniqueness of a fingerprint is determined by the local ridge characteristics and their relationships. The two most prominent local ridges called minutiae. The first is defined as the point is a ridge or branch ridges. A good quality fingerprint are contains about 40 to 100 minutiae points. Fingerprint recognition, is pattern recognition, and is used in security to identity authentication service. Fingerprint matching has three different Categories, Ridge feature Based, Correlation Based, namely, and Minutiae Based. Minutiae based fingerprint matching is the most widely used fingerprint matching, and this is minutiae based. The minutia extractor, a three stages are widely used by researchers. These stages are minutiae extraction, preprocessing, and post processing. Fingerprint recognition, is an application in pattern recognition, and is used in security to identity authentication. Fingerprint matching has three different Categories, namely, Correlation Based, Minutiae Based, Ridge feature Based. Minutiae based fingerprint matching is the most widely used fingerprint matching algorithm, and this algorithm too is minutiae based processing.

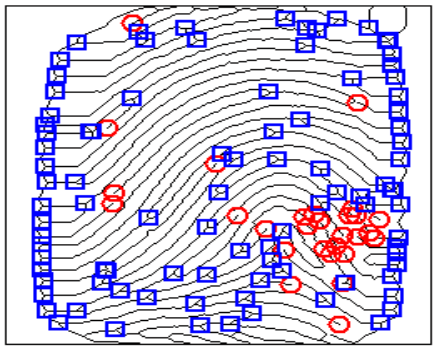

Fig 3: Minutiae Points.

A fingerprint is a series of ridges and furrows on the surface of the finger. Pattern of ridges and furrows as well as minutiae can be used to determine the uniqueness of fingerprint. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. Fingerprint is preprocessed to remove the noise and irrelevant information.

d) Combined Fingerprint Minutiae Template Generation:

The Combined Fingerprint Template is generated by combining the minutiae points extracted from the first fingerprint and the orientation field extracted from the second fingerprint. The combined fingerprint template is generated for various combinations of fingerprints. The templates can then be stored in a database which can be used as a reference during the authentication.

III. OVERVIEW OF THE SYSTEM

MANETs are a type of wireless networks which are rapidly growing because there is no such requirement for setting up an infrastructure for their operational purposes. In such networks, the topology is dynamic, and the nodes are mobile in nature. It must be able to continue their traffic even if the wireless transmission medium is out of range. A nodes travel often, it won't be having an unchanging infrastructure as a result it is unsafe and will be inclined by various attacks. Each node has a finite interaction range, which will be behaves as a router to communicate the packets to another node. DOS (Denial-of-Service) attack, Flooding attack are some serious threats in MANET which causes data unsafety in MANET. The main problem in MANET is that, the routing tables which consists of each neighbour node information which maintained by the each node for the dynamic topology creation which is insecure. An optimized FMNK (Finger print Minutiae point non-invertible Key) algorithm is produced utilizing Biometric image models are introduced which can afford security and authentication. An optimized FMNK-SSL-AES-256(Finger print non invert able key Secure Socket Layer-Advance Encryption Standard) encryption algorithm is being introduced to encrypt the information applying a key to increase the security in MANET. Intra-cluster routing involves routing within a cluster. Each node maintains routing information about its cluster. A clustering architecture provides network scalability and fault tolerance, and results in more efficient use of network resources. It can be used for resource management, routing and location management to reduce communication and computational overhead. In this section, we discuss cluster formation and maintenance mechanisms. Cluster head election algorithms have been proposed for mobile ad-hoc networks (MANET) that assume link steadiness, mobility, connectivity, cluster and weight are therefore closely related to our work.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (303-314), Month: October - December 2015, Available at: www.researchpublish.com

IV. DESIGN

The proposed system is to develop the secure communication among nodes. An optimized FMNK algorithm is developed utilizing Biometric fingerprint and complication is increased, which can provide more security with minimum time complexity by reduction of the number of rounds and key generation time and it provides a strong authentication mechanism. And it also increases the security level in MANET with application of SSL-AES-256 (Secure Socket Layer-Advance Encryption Standard) encryption algorithm model with FMNK key. The minutiae points are generated from the receivers finger print and transformed into cancelable template. After shuffling cancelable template, two points cross over genetic point is applied and non-invertible key is generated.

a) FMNK algorithm:

The method of obtaining the transformed points from minutiae points and Creating optimized FMNK algorithm.

ALGORITHM:

Algorithm: Creating a FMNK algorithm

Input: Fingerprint, Minutiae points

Output: FMNK algorithm

Step1: Take the A-axis and B-axis of the fingerprint to extract the minutiae Points, represented as

$M_P = \{Pi\}$ where i = 1.....n (1)

Step2: The A, B coordinates are now converted and stored as a vector. The resultant vector is represented as

$M_v = [A_1B_1\ A_2B_2\ A_3B_3\ .....A_nB_n]$ (2)

Step3: Now, the next sequential prime number of each value in the vector M_v should be evaluated and it is saved in vector NP_V

$NP_v = [A^1{}_1B^1{}_1\ A^1{}_2B^1{}_2\ A^1{}_3B^1{}_3\ .....A^1{}_nB^1{}_n\ ]$ (3)

Step 4: Now, substitute the values of M_v and NP_v in the formulae

$DE = 2^{Mv(i)} \bmod NP_{v(i)}$ where i = 1 ..... n (4)

Step 5: Further, calculate the next sequential prime no which is appended to CPDE

CPDE << { CPDE(t), if (DE(t) = prime)

Next prime, otherwise

$CPDE = [PA_1PB_1\ PA_2PB_2\ PA_3PB_3.....PA_nPB_n]$ (5)

Step 6: The next step includes assessing the position of the prime number, which is done by replacing the value of CPDE through the step 5 and s value

Pos (|CPDE|-s) where s = 0, 2, 4, 6,...|CPDE|

Step 7: The resultant position number is saved in the transformed point vector denoted as

$TP = [P_1\ P_2\ P_3\ P_4.....P_n]$ (6)

Step 8: Find the distance among the each point using the formulae

$Distance\ (P_t, P_j) = \sqrt{(A_t - A_j) + (B_t - B_j)}$ (7)

As a result, a 256-bit key will be generated

Step 9: Now, sorting operation which is employed so as to sort the values in ascending order which resulted is represented as

$K_D = K\ sort = [K_{D1}K_{D2}\ K_{D3}.....K_{Dn}]$ (8)

Step 10: The UD are divided into 2 equal parts represented as

$K_{D1} = [K_{D1}\ KD2..... K_{Dn/2}]$ (9)

$K_{D2} = [K_{Dn+1\ KD2} .....K_{Dn}]$ (10)

Where all values in the parts KD1 and KD2 are assigned indexes respectively.

Step 11: All even index positions are saved at odd positions of OPU2 and all odd positions are saved at the even positions of EPU1

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (303-314), Month: October - December 2015, Available at: www.researchpublish.com

Step 12:"Genetic Two Point Crossover" operation is applied on EPU1 and OPU2 and are integrated, which can be represented as $GTCK_D$

$GTCK_D$ = twopointcrossover [EPK1, OPK2] (11)

Step 13: Binary vector key is generated using the following formula

$K[t] = GTCK_D[t] \bmod 2$ where $0 < t < 256$ (12)

Step 14: Consider any string with 32-bit size and perform an XOR operation with K[t]

The FMNK key is generated is used to encrypt the information using optimized SSL-AES-256 algorithm. AES algorithm provides highest security levels compared to the other encryption algorithm because of its large key size.

b) FMNK with AES-256 Algorithm:

The AES structure is data block of 4 columns of 4 bytes is state.It key is expanded to array of words has rounds in which state undergoes:

- byte substitution (1 S-box used on every byte)
- shift rows (permute bytes between groups/columns)
- mix columns (subs using matrix multiply of groups)
- add round key (XOR state with key material)
- view as alternating XOR key & scramble data bytes

A simple substitution of each byte uses one table of 16x16 bytes containing a permutation of all 256 8-bit values. The XOR state with 128-bits of the round key. Again processed by column (though effectively a series of byte operations) inverse for decryption identical since XOR own inverse, with reversed keys.

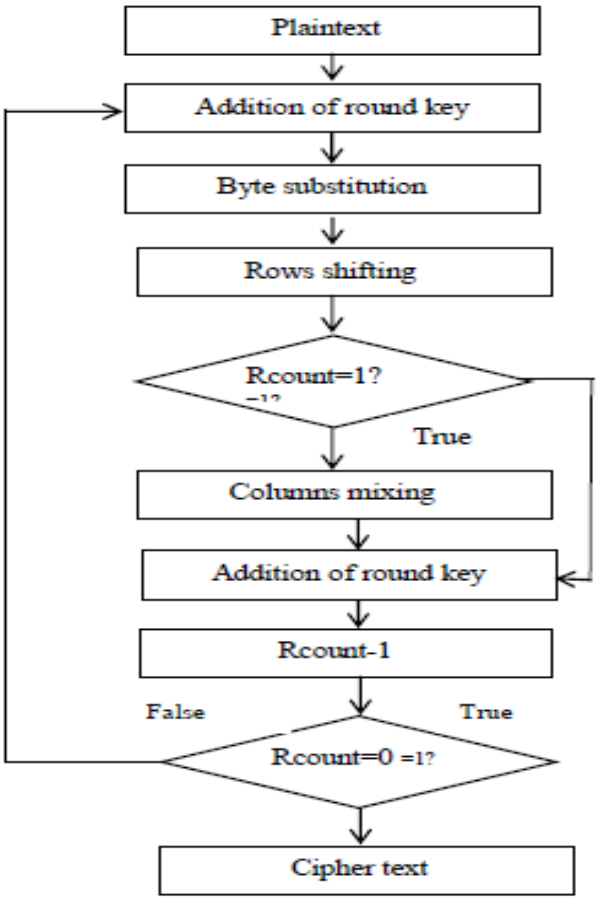

Fig 4: AES-256 Algorithm

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (303-314), Month: October - December 2015, Available at: www.researchpublish.com

The minutiae points are generated from the receivers finger print and transformed into cancelable template. After shuffling cancelable template, two points cross over genetic point is applied and non-invertible key is generated. The sender's watermarked face image attached to data and encrypted using generated cryptographic key. At the receiver side reverse process takes place. Receiver's fingerprint is used for the decryption. The senders face is extracted and watermarked image checked for the authentication. A fingerprint is made of a series of ridges and furrows on the surface of the finger.

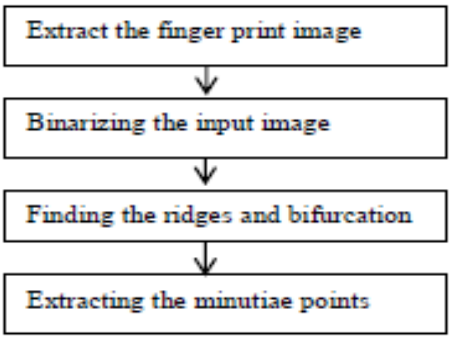

Fig 5: Minutiae Point Extraction Algorithm.

Inter and intra-Cluster Routing

It describes the inter-domain routing protocol of IDRM in pseudo codes. We present three algorithms to be executed at each gateway. Algorithm 1 is a subroutine to generate a new route announcement. Algorithm 2 is a continual process of a gateway to handle the interaction between inter-domain gateways. Algorithm 3 is a continual process to manage the intra-domain membership. For a gateway i in a domain A, let $G^{intra}(i)$ denote a set consisting of the intra-domain gateways to that i has connectivity, and $G^{inter}(i)$ denote a set consisting of the inter-domain gateways i is directly connected. Let M(i) denote the set of intra-domain members to that i has connectivity. The node IDs are unique throughout the entire MANETs. In practice, each MA-NET will typically belong to an organization, which will have an address space pre-assigned or allocated on-demand from a centralized entity. There is a naming service similar to DNS that translates a name to an ID. When a sender wants to send a packet to a destination, it can obtain the ID of the destination. The communications between inter-domain gateways are bidirectional, and the gate-ways can support multiple radio access technologies to enable the communications among different domains. A non-gateway node is always willing to forward packets for intra-domain nodes, but not necessarily for other inter-domain nodes.

Algorithm 1 Route Announcement Generation

if (any change in $G^{intra}(i)$) then
  // generate a new MANET ID
  MANET ID ← f(A, $G^{intra}(i)$)
 // else MANET ID does not change
end if
if (any change in M(i)) then
  // generate a new membership digest
  MD ← b(M(i))
  // else the membership digest does not change
end if
path ← {MANET ID}
return a new route announcement [MD, path]
Algorithm 1 checks any change in the membership of $G^{intra}(i)$ and M(i)

In the route announcement, path is an ordered list of MANET IDs, i.e., [MANET ID_1, . . ., MANET ID_n], which indicates the nodes in MD can be reached by traversing MANET ID_1, then MANET ID_2, . . ., and finally MANET ID_n announcement is already in its list of neighbours. When it processes a route announcement, it first examines if the origin

of the announcement is already in its list of neighbours. If it is a new neighbour it updates the list. The uniqueness of a fingerprint is exclusively determined by the local ridge characteristics and their relationships. The two most prominent local ridge characteristics, called minutiae, are the ridge ending and the bifurcation ending and the ridge bifurcation.

Algorithm 2 Main Routine of the Gateway

```
while (true) do
  if (timer > announcement interval) then
     // generate a new route announcement
     call Algorithm 1
     send the route announcements to G^inter(i)
  end if
  if (received a route announcement [MD, path]) then
    if (announcement from g^new not in G^inter(i)) then
       // new connected inter-domain gateway found
       G^inter(i) ← G^inter(i) ∪ {g^new}
     end if
  if ((no route to MD) OR (path ≺ route to MD)) then
       // update the path vector
       insert [MD, path] at the top
       path ← append (MANET ID, path)
       announce [MD, path] to G^inter(i) ∪ G^intra(i)
  end if
end if
increment timer and sleep
end while
```

Algorithm 2 presents the main function of a gateway participating in IDRM. The main routine consists of two parts. First, it periodically polls its domain status, generates a new route announcement, and broadcasts a route announcement to its neighbouring inter-domain gateways. Second, it wakes up when a new route announcement is received from one of its neighbours and processes them. Also, a domain of MANET can be partitioned into disjoint networks without direct intra-domain connectivity, and the intra-domain connectivity may only be maintained by traversing the nodes in other domains. These properties impair the direct application of a traditional inter-domain routing protocol to MANETs.

Algorithm 3 Beaconing among Intra-domain Gateways

```
while (true) do
    if (timer > beacon interval) then
        send beacons to every gateway in Gintra(i)
    end if
  for all (gateway g in G^intra(i)) do
     if (no beacons from g within time limit) then
         // network has partitioned
         G^intra(i) ← G^intra(i)\{g}
         raise change flag
     end if
   end for
      if (received a beacon from g not in G^intra(i)) then
         // network merge event OR new gateway
```

$G^{intra}(i) \leftarrow G^{intra}(i) \cup \{g\}$
raise change flag
end if
if (change flag is up) then
// generate a new route announcement
call Algorithm 1
send the route announcement to $G^{inter}(i)$
reset change flag
end if
increment timer and sleep
end while

Algorithm 3 is a separate thread that takes care of the exchange of beacons among the gateways in the same domain. Periodically, a gateway sends out a beacon to all intra-domain gateways notifying its presence. When it does not receive a beacon from one or more of the gateways in its intra-domain, it updates $G^{intra}(i)$. Similarly, when it receives a beacon from a gateway g that is not currently in the list of intra-domain gateways, it updates its entry. When these changes are detected, the gateway initiates a route announcement process to update its neighbours.

Cluster Formation:

All the members reachable by this new Local Controller will form a new cluster. If group members that exist and do not belong to the formed clusters then choose the nodes that have the maximum reachability to the others nodes in one hop from the remaining members.

The AODV is one of the reactive routing protocols most commonly used in MANETs. Although the AODV protocol performs well with mobile nodes, it incurs high overhead with an increase in the network's size, the nodal degree or the number of communicating source-destination pairs. By using AODV route construction and maintenance mechanisms, clustering architecture can be constructed on demand. Clusters are maintained when data are to be sent.

The Step by step Pseudo code of the present work is as follows

1. Start
2. Create a network.
3. Formation of cluster.
4. Evaluating the Cluster Head.
5. Using Cluster - AODV routing protocol, synthesis of network which introduces less overhead that the pure AODV protocol without clustering.
6. End.

The Clustering Based Routing approach provides a solution for decrease routing control overhead and improves the network scalability. In CBR, group a node into clusters in each cluster one node act as a cluster heads in order to reduce the communications and control overheads.

IMPLEMENTATION:

The proposed scheme can be simulated in ns-2 simulator with the optimized FMNK algorithm and FMNK with AES-256 Algorithm. Performance analysis of the proposed extension Using the AES-256 Encrypt/Decrypt time to FMNK the process is done in lesser time when compared to AES-256 Encrypt/Decrypt time without FMNK. So, in this way it is proved that AES-256 Encrypt/Decrypt time with FMNK does the process in lesser time.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (303-314), Month: October - December 2015, Available at: www.researchpublish.com

TABLE I. Simulation Parameters

Parameters	Value
Transmission range	250m
Topology Size	1000*1000
Simulation Time	100s
Packet size	512 bytes
Traffic type	CBR
Routing protocol	AODV
Number of nodes	10,20,30
Antenna Type	Omni Antenna
Propagation	Two Ray Round
MAC protocol	IEEE 802_11

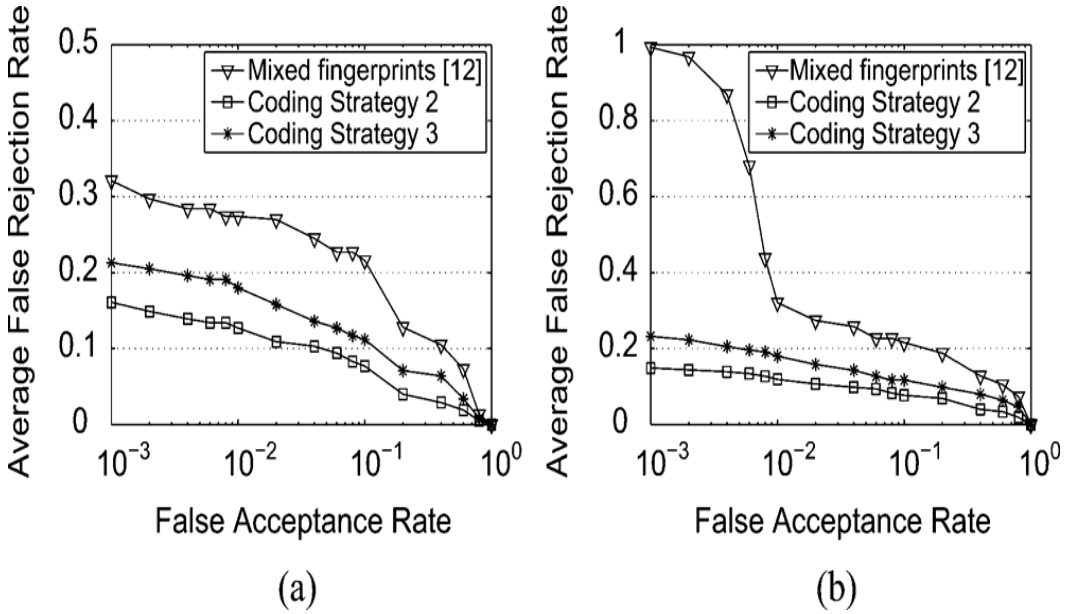

Fig 6: Performance comparison between the combined fingerprints and the mixed fingerprints

Fig 7: Simulation for cluster formation

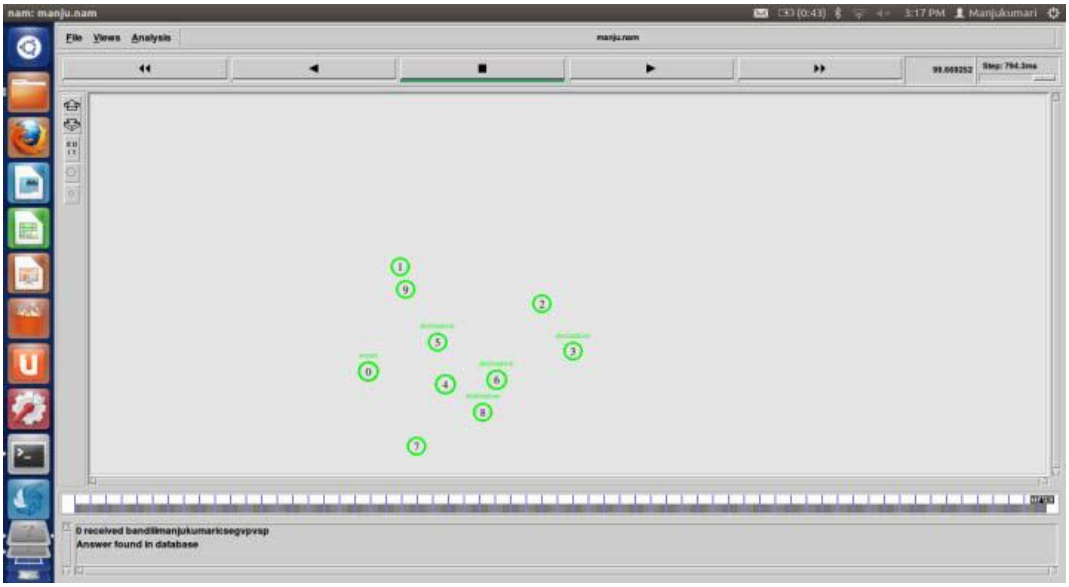

Fig 8: Simulation for secure message passing from source to destination

V. CONCLUSIONS

In this paper, propose an optimized FMNK (Finger print Minutiae point non-invertible Key) algorithm is produced utilizing Biometric image models are introduced which can afford security and authentication. An optimized FMNK-SSL-AES-256(Finger print non-invertible key Secure Socket Layer-Advance Encryption Standard) encryption algorithm is being introduced to encrypt the information applying a key to increase the security in MANET Routing table. A clustering architecture improves the networks scalability and fault tolerance, and results in a more efficient use of network resources.

REFERENCES

[1] S. McLaughlin, D. Laurenson, and Y. Tan, 'Mobile ad-hoc network', Aug. 10 2006, US Patent App. 11/351,777. [Online] Available: http://www.google.com/patents/US20060176829.

[2] KruahanedoBeloro, 'Intrusion Detection System On Mobile Ad Hoc Network' ASM e-International journal, e-ISSN-2320-0065.

[3] N. Lalithamani and K.P. Soman, 'An Efficient Approach For Non-Invertible Cryptographic Key Generation From Cancelable Fingerprint Biometrics', International conference on Advances in Recent Technologies in communication and Computing, 2009. 978-0-7695-3845-7/09 © 2009 IEEE Pg.47-52.

[4] V. Sunil, K. Gaddam, ManoharLal, 'Efficient Cancelable Biometric Key Generation Scheme for Cryptography', International Journal of Network Security, Vol: 10, No: 3, pp: 223-231, 2010.

[5] M.P. Mehta, H .Diwanji, J. S. Shah, 'A Genetic Based Non-Invertible Cryptographic Key Generation from Cancelable Biometric in MANET', Int. J. Comp. Tech. Appl., Vol 2 (6), 3019-3022, NOVDEC 2011.

[6] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M .Bolle, 'Generating cancelable fingerprint templates'. IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(4):561–572, 2012.

[7] S. Pankanti, S. Prabhakar, A.K. Jain, 'On the individuality of Fingerprints', IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 24, No. 8, pp.1010–1025, 2002.

[8] Vladimir D. Orlic, MiroslavPeric, ZoranBanjac and SasaMilicevic 'Some aspects of practical implementation of AES 256 crypto Algorithm', Serbia, Belgrade, November 20-22, 2012, 20th Telecommunications forum TELFOR 2012.

[9] Md. Abdullah-Al-Mamun, M. MahbuburRahman and Hwee-Pink Tan, 'Performance Evaluation of TCP over Routing protocols for Mobile Ad Hoc Networks', Communications and Networking in China, 2011. First International Conference on DOI:10.1109/CHINACOM.2006.344668.

[10] M. A. Fischler, R. C. Bolles. Random Sample Consensus, 'A Paradigm for Model Fitting with Applications to Image Analysis and Automated Cartography', Vol24, pp 381-395, 2012.

[11] Mehta ManishaPravinchandra, HiteishiMilindDiwanji and Jagdish Shantilal Shah and HemaliKotak ,'Performance Analysis of Encryption and Decryption using Genetic Based Cancelable Non-Invertible Fingerprint based Key in MANET' , 2012 International Conference on Communication Systems and Network Technologies, 978-0-7695-4692-6/12 $26.00 © 2012 IEEE DOI 10.1109/CSNT.2012.84. www.crypto.com.

[12] Alekha Kumar Mishra, Bibhu Dutta Sahoo, 'Analysis Of Security Attacks For AODV Protocol In MANET', Proceedings of National Conference on Modern Trends of Operating Systems, MTOS-2009, page 54-57.

[13] K. Tamizarasu, M .Raja ram, 'An AODV-based Clustering Approach for Efficient Routing in MANET', International Journal of Computer Applications (0975 – 8887) Volume 51– No.15, August 2012.

[14] N.Radha, S .Karthikeyan, 'An Evaluation Of Fingerprint Security Using Noninvertible Bio hash' ,International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011.

[15] Guruprakash.V, Arthur Vasanth. J, 'Combined Fingerprint Minutiae Template Generation', International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014.

[16] Shubha Mishra and Dr. Manish Shrivastava,' Efficient Secure Clustering Protocol for Mobile Ad-Hoc Network', Journal of Global Research in Computer Science, Volume 2, No. 9, September 2011.

[17] Prabhakara Rao .T and Gintanjali Sahu, 'Protecting Fingerprint Privacy Using Combined Minutiae Template Generation Algorithm', (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3), 2015, 2290-2294.

[18] Chi-Kin Chau, Jon Crowcroft, Kang-Won Lee, Starsky H.Y. Wong, 'IDRM: Inter-Domain Routing Protocol for Mobile Ad Hoc Networks' UCAM-CL-TR-708 ISSN 1476-2986, January 2008.

AUTHOR'S BIOGRAPHY

Parameswaran.T has received his B.E degree in Electronics and Communication Engineering from Velalar College of Engineering and Technology, Erode, and M.E degree in Software Engineering from College of Engineering Guindy, Anna University Chennai in 2005 and 2008 respectively. He is currently pursuing his Ph.D Anna University Chennai. He is currently working as Teaching Fellow in the Department of Computer Science and Engineering, Anna University Regional Campus, Coimbatore, Tamilnadu, India.

Palanisamy.C has received his B.E degree in Electronics and Communication Engineering from University of Madras, Chennai and M.E degree (Gold Medalist) in Communication Systems from Thiagarajar College of Engineering, Madurai, Madurai Kamaraj University in 1998 and 2000 respectively. He has received his Ph.D from the faculty of Information and Communication Engineering, Anna University, Chennai in 2009. He has more than 15 years of academic and research experience and currently he holds the post of Professor and Head of the Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India. He has published more than 40 research papers in various journals and conferences. He has organized more than 15 workshops and holds 2 funded projects. He is a lifetime member of ISTE. He Won Best M.E Thesis Award at Thiagarajar College of Engineering, Madurai and best paper award titled, "A Neural Network Based Classification Model Using Fourier and Wavelet Features," Proceedings of the 2nd Int. Conf. on Cognition and Recognition 2008, (ICCR 2008), Organised by P. E. S. College of Engineering, Mandaya, Karnataka, India, pp. 664-670, 2008. His research interests include Data mining, image processing, and mobile networks.

Elankathir.E has received his B.E degree in Computer Science and Engineering from Sri Bharathi Engineering College for Women. She is currently pursuing her M.E degree in Software Engineering from Anna University Regional Campus, Coimbatore. Tamilnadu, India.