SUSTAINING SECURITY IN MANET THROUGH BIOMETRIC TECHNIQUE INCULCATING META-HEURISTIC ALGORITHM

SHERIN ZAFAR, DR.M.K SONI

Abstract: The paper comprehends an impending accost of intensifying biometric stationed authentication technique bestowing meta-heuristic 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 as they are 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 meta-heuristic algorithm to overcome the security and privacy concerns that exist in biometric technology. The foremost requirement of our this technique is to overcome various data attacks such as wormhole, cache poisoning, invisible node attack etc. that are confronted by MANET and hence make the network more secure.

Keywords: Biometrics, BKG(biometric key generation) process, meta-heuristic algorithm, secure routing protocols in MANET.

Introduction: An ad-hoc network is integrated robustly from scratch manipulating wireless connections and composed of mobile nodes. 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. These security demands lead to the advancement of various secure protocols for routing in MANET that aim to protect the network and hence enhance its performance. 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 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[11] .We discuss the prevailing secure routing protocols in MANET and how their discrepancies can be avoided by proposed impending authentication technique for MANET.

- ***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.
- ***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).
- ***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.[10].

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

Necessity of Biometrics Security: Biometrics, 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. 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.

Meta-heuristic Algorithms: 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)

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 .

Anand Patwardhan et al. [2] 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.

Abhishek Roy and Sajal K Das.[1] 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.

Shanthini.B etal.[22]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.

Prospective Work: In the recommended biometric stationed authentication technique bestowing meta-heuristic algorithm, any one of the meta -heuristic algorithm like GA, ANN, simulated annealing etc 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 , meta-heuristic algorithm and cryptography hence providing authentication and thus enhancing network performance .In the prospective protocol every node in MANET cultivate biometric impressions of each and every other node. Prospective technique will exploit strong biometric. If a source node transfers a message to any destined node, the source undergoes biometric key generation process. Biometrics are refined to align the scale and radiation. Then follows feature evulsion and application of meta-heuristic algorithm which results in generating cryptographic key by employing either Fiestel or DES key generation algorithm for the technique. Receiver exploits his biometric to institute the corresponding cryptographic key and the similar 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.

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

Cipher-text=Encryption Algorithm BK (Plaintext)

Plaintext = Decryption Algorithm BK (Cipher-text)

where:

BK - Biometric Key (created by Recipient Biometric)

In Fiestal algorithm, a block of size N is divided into two halves, of length N/2, the left half called XL and right half called XR. The output of the ith round is determined from the output of the (i-1)th round. The same key is used for all iterations without generating sub keys. Also the number of iterations performed is reduced to show that security can be achieved by using simple algorithm as specified in fig.1.

- **Authentication:** Through the proposed technique, 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.

- **Integrity:** Integrity is maintained in this technique 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.

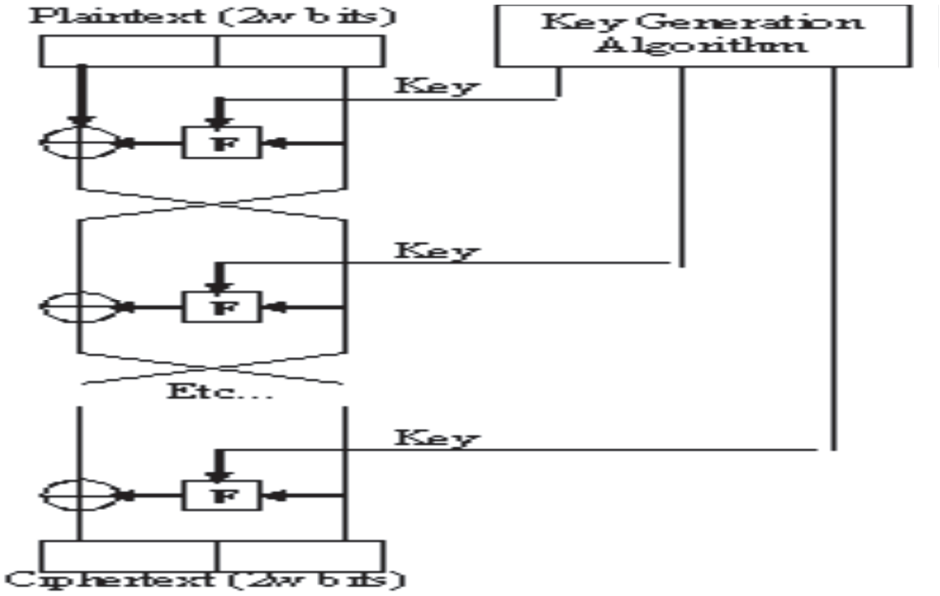

Fig 1. Fiestal Algorithm

Simulation Workflow: Implementation of the proposed technique will be done through MATLAB platform and analysing the simulations through NS2.The proposed protocol will be compared with the previous secure protocols like SEAD ,SAR ,SRP etc and performances will be evaluated through various features like reduced overhead, enhanced levels of security, key size and time consumed in key generation, encryption and decryption of data etc .

Conclusion And Future Work: The paper, focuses on sustaining security in MANET through biometric stationed authentication technique inculcating meta-heuristic algorithm.First phase of the technique generates strong biometric features which undergoes a biometric key generation(BKG)process .A crypt-biometric 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 of the technique will be dependent on the simulation results being analysed.

References:

1. 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.
2. Anand Patwardhan, 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.
3. 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.
4. Awerbuch.B et al., "Ad hoc On-Demand Distance Vector Routing Protocol Resilient to Byzantine Failures", ACM Wise, 2002.
5. D.E. Goldberg, "Genetic Algorithms in Search, Optimization and Machine Learning" Addison Wesley, New York, 1989.
6. Farooq Anjum, Dhanant Subhadrabandhu and Saswati Sarkar "Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols"

in proceedings of IEEE 58th conference on Vehicular Technology, 2003.
7. Fessi B A, Ben Abdallah, 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.
8. Guerin.R.A and A. Orda, Q0S routing in networks with inaccurate information: Theory and algorithms,IEEE/ACM Transactions on Networking 7(3) (1999) 350–364.
9. Haas.Z, J. Deng, B. Liang, P. Papadimitratos and S.Sajama Wireless ad hoc networks. In J. Proakis, editor, Wiley Encyclopedia of Telecommunications.John Wiley and Sons, 2002.
10. Hahill.B et l., "A Secure Protocol for Ad Hoc Networks", OEEE CNP, 2002.
11. Hao.Y et al., "Security In Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, 2004.
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, December, 2009.

* * *

Facult of engineering ,Professor, Dept.of Computer Science & Engg
Manav Rachna International University Faridabad, India
Sherin_zafar84@yahoo.com, ed.fet@mriu.edu.in