RESEARCH ARTICLE OPEN ACCESS

Secure Cluster Based Routing Using SAT/ILP Techniques and ECC EL-Gamal Threshold Cryptography in MANET

Mr. P. Kanagaraju. Me, (Ph. D)*, Dr. R. Nallusamy Ph.D.**, Nandini. D. K***
*Department of Computer Science, K.S.Rangasamy college of Technology, Thiruchengode
** Professor
***Department of Computer Science, K.S.Rangasamy college of Technology, Thiruchengode.

ABSTRACT
The Elliptic curve cryptography (ECC) a promising and important because it requires less computing power, bandwidth, and also the memory when comparing to other cryptosystems The clustering algorithm using the Integer Linear Programming (ILP) and Boolean Satisfiability (SAT) solvers. These improvements will secure the application of SAT and ILP techniques in modeling composite engineering problem that is the Clustering Problem in Mobile Ad-Hoc Networks (MANETs). The Clustering Problem in MANETs consists of selecting the most appropriate nodes of a given MANET topology as clusterheads, and ensuring that regular nodes are related to clusterheads such that the lifetime of the network is maximized. In which, discussing SAT/ILP techniques for clustering techniques and ECC El Gamal Threshold Cryptography for the security. Through our implementation, explored the possibility of using ECCEG-TC in MANETs.

***Keywords* -** Boolean Satisfiability, Elliptic curve cryptography, ECC El Gamal Threshold Cryptography Integer Linear Programming.

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are vulnerable to various attacks including denial-of-service attacks because of wireless nature of these networks. Devices with constraint resources add to its vulnerability. To ensure availability of nodes, threshold cryptography can be implemented in these networks so that even if some of the information is lost still the actual message reaches the intended receiver without compromising security in terms of secrecy, reliability, and genuineness.

Elliptic Curve Cryptography (ECC) was first proposed by victor Miller and independently by Neal Koblitz in the mid-1980s and has evolved into a mature public-key cryptosystem. Distinguish to its conventional counterparts, ECC offers the same level of security using security.

Threshold cryptography achieves the security needs such as confidentiality and integrity against malicious nodes. It also provides data integrity and availability in a hostile environment and can also employ verification of the correct data sharing. All this is achieved without revealing the secret key. Thus, taking into consideration these characteristics, implementing TC to secure messages seems a perfect solution in MANETs.

For the past few decades, Integer Linear Programming (ILP) and Boolean Satisfiability (SAT) solvers have enhanced a lot through the beginning of new intelligent algorithms that allowed the solvers to handle a wider range of difficult Engineering based problems. Mainly one of such problem is clustering in Mobile Ad-Hoc Networks (MANETs). Cryptography is transforming a information it into an unreadable format in which a message can be concealed from reader and only the intended recipient will be able to convert it into original text. Its main goal is to keep the data secure from unauthorized access. Data can be read and understood without any special measures are known as plaintext. Hiding information into the plaintext is called encryption. Encrypted plaintext information into an unreadable garbage known as cipher-text. Reverting process of cipher text to its original plaintext is called decryption. A system provides encryption and decryption is called cryptosystems. Cryptography provides number of security goals to ensure the privacy of data, on-alteration of data and so on. Types of various goals of cryptography are below

Confidentiality

Maintaining a secret communication between the two authorized persons.

Authentication

Checking the identity of the information from the legitimate or authentication ID.

Data Integrity

Verifying the information that has not been altered by unauthorized which means no one in between the sender and receiver are allowed to alter the given message.

Non Repudiation

Thus when a message is sent, the receiver can prove that the message was in fact send by the suspected sender. Correspondingly, when a message is received, the sender can prove the suspected receiver in fact received the message.

Access Control

Only the certified parties are able to right to use the given information

.

II. Integer Linear Programming And Boolean Satisfiability

Integer Linear Programming (ILP) involves maximizing or minimizing a function with respect to certain constraints where the optimal function and constraints are linear and the used variables can only take integer values [2]. Cases where the integer values are restricted to (0–1) are called Binary ILP Problems. In SAT the constraints between variables are represented using what is called propositional logic. It involves the use of AND, OR and NOT operations to construct formulas in the Products-of-Sums form or Conjunctive Normal Form (CNF). The variables can only take Binary values (0–1). Given constraints articulated in CNF, the ambition is to spot a variable obligation that will satisfy all constraints in the problem or verify that no such task exists. To assure or to solve, SAT will go all the way through the hunt space and conclude whether or not there is a fulfilling variable assignment. Superior decision heuristics and clever inconsistency analysis techniques can be used to evade probing through the complete tree of 2*n* assignments.

It proposes an ILP formulation of the clustering problem, structure on the ideas and assumptions put forward in the EEC-CB model presented in this model improves on weaknesses present in the EEC-CB model and adds idleness through the use of a Star-Ring backbone. In addition, a proposed enhancement allows coverage to be taken into account.

Proposed Base Model

Variables are maintained below as:

- N: Total number of nodes in the network (predetermined)
- P: Number of clusters heads (predetermined)
- $d_{i j}$: Euclidean distance between nodes i and j
- K : Max number of nodes that can be connected to a CH (predetermined)
- $c_{i j}$: Cost of connecting a regular node i to CH j (proportional to $d_{i}^{2}{}_{j}$)
- $h_{j k}$: Cost of connecting CH j to CH k (proportional to d^{3}_{jk})

The assumptions which were made above in the ILP formulations are also valid to the proposed ILP formulation. Variable *b*, in the intention role, which represents the level of the node's capability to act as a cluster head, gets its value from an external source (algorithm, tool, etc). This is useful as multiple approaches or algorithms, which decide the suitability of a node in acting as a cluster head, can be combined with this model without altering the equations, even though this is out of the range of research. Then it is unspecified that nodes are able to resolve each other's spot.

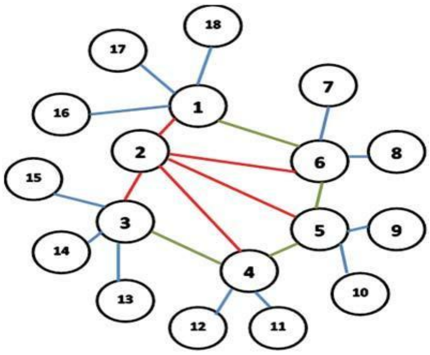

Fig. 1 Star-ring backbone.

Intra Cluster Communication Enhancement

Intra Cluster communication is introduced for two issues. First is that the most important accountability of the cluster head should be to route communication among clusters and not inside a cluster. The aim is for the cluster head to preserve as much energy as achievable for the contact between clusters, allowing it to last longer in its position as a cluster head. The second cause after enhancing the intra cluster contact is that should a cluster head fail, the nodes inside a cluster will be able to communicate.

Multihop Connections Enhancement

Multihop connections are introduced into the formulation to permit longer, extra exclusive links to be replaced by shorter less costly links. relatively than attach straight to a cluster head which is further away, it is preferable to make a lesser cost link to a cluster head during another regular node. Though, the in-between regular node will now, in a sense, act like a second tier cluster head as it will route the communication of the regular node through it to the cluster head. Price of this routing must be taken into explanation. After that objective function is used to integrate the cost of multihop connections to the proposed Star-Ring base model.

Coverage Enhancement

The proposed Base Model can be extended to take into account the coverage radius of the nodes in the system, and make sure that links are recognized only between nodes that are within each other's exposure radius. Likewise the same manner in which the distances between nodes are used to determine the price of the links, it can also be compared to the exposure radius of each node and used to Sample MANET topology.

III. Ecc Elgamal Tc (Ecceg-Tc)

The ELGamal public-key encryption scheme can be viewed as Diffie-Hellman key agreement protocol in key transmit mode. Its protection is based on the intractability of the discrete Logarithm Problem (DLP) and the Diffie-Hell man problem.
EC-ELGamal protocol implemented for safe communication. One essential tip is to note is unlike ECDH protocol, this protocol does not create common key, but using EC-ELGamal protocol a message M=(M1,M2),a point on elliptic curve, can be sent from Bank to Alice and vice versa.

Performing the decrypting, reverse the embedding process to create the message M starting to the point P. It is not trivial to find a point M for the communication. Communication that is difficulty in obtaining the private key from the public key is based on the discrete log problem (DLP) for elliptic curves.

The ELGamal digital signature scheme:

The ELGamal signature algorithm is similar to the encryption algorithm in that the public key and private key have the same form; however, encryption is not the same as signature verification, nor is decryption the same as signature creation as RSA.
In following sections, our goal is to implement ECC based ElGamal threshold cryptography (ECCEG-TC). In this algorithm, key is not shared because the public as well as private keys are in form of points and we cannot apply Lagrange on the points altogether to split message or to combine it. Hence, ECCEG-TC for message splitting before encryption is simulated for MANET environment and then it is compared with performance of RSA-TC. The ECC El Gamal Threshold cryptography (ECCEG-TC) algorithm is briefly explained.

ECCEG-TC Message Split before Encryption Algorithm

Suppose that the ECC has a point G on an elliptic curve $E_p(a, b)$, and the order of G is q. p is a large prime.
Bob's private key and public key are n_B, $0 < n_B < q$, and $K_B = n_BG$.

- First we choose a prime number $p > max(M, n)$, and define $a_0 = M$, the message. Then we select $k - 1$ random, independent coefficients $a_1, a_2,...a_{k-1}$, $0 \leq a_j \leq p-1$, defining the random polynomial $f(x)$ over Zp, a Galois prime field $GF(p)$.
- We compute n shares, $M_i = f(x_i) \bmod p, 1\leq i \leq n,$ *where* x_i can be just the public index i for simplicity, and convert them to points P_i on elliptic curve $E_p(a, b)$.
- Alice picks a random number r, and sends rG and $P_i + rK_B$ to Bob with index t.
- Bob recovers each elliptic curve point by calculating $P_i + rK_B - n_BrG = P_i$.
- Bob converts P_i to M_i, and deduces M by using Lagrange interpolation formula M.

ECCEG-TC Implementation

ECCEG-TC,to select the ECC parameters, i.e. *a*, *b*, *p*, widely accepted NIST curves were selected for implementation for *192*, *224*, and *256* bits. For conversion of message to and from ECC point, method discussed by Kobiltz is used such that $(kappa*M)mod\ p < x <(kappa*(M+1))mod\ p$, *where* (x, y) is a point on elliptic curve. In our ECCEG-TC implementation, *kappa* is fixed to 2^8. To retrieve a message from a ECC point (x, y), $M= x/kappa \bmod p$ is used.

For calculating the shares and for combining partial messages, Shamir's Lagrange interpolation scheme is implemented. For its polynomial, the coefficients are randomly generated over the *modulus p*. The co-efficient zero depends on the *x* and *y* values of ECC point information that needs to be transmitted based on ECC algorithm used. As against RSA algorithm where we are sharing the keys, in ECC-TC implementation, the partial shares of the message are generated and then encrypted to get ECC point.
Cryptography is transforming a information it into an unreadable format in which a message can be concealed from reader and only the intended recipient will be able to convert it into original text. Its main goal is to keep the data secure from unauthorized access.

IV. Performance Results Performance Results

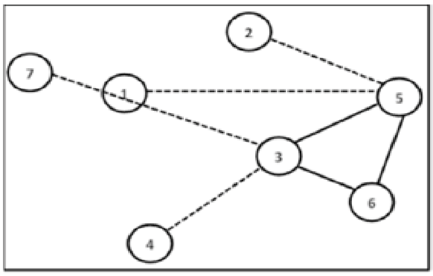

Fig. 2 Topology generated by the ILP formulation without coverage constraints.

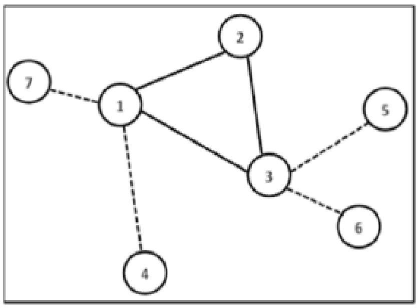

Fig. 3 Topology generated by the ILP formulation with coverage constraints.

Fig.4 illustrates that with increase in ECC key size, the total encryption timings increase gradually for given *n* and *t*. For constant key size and *n*, the encryption timings increase with *t* as the time to generated Lagrange polynomial and respective message shares increases accordingly.

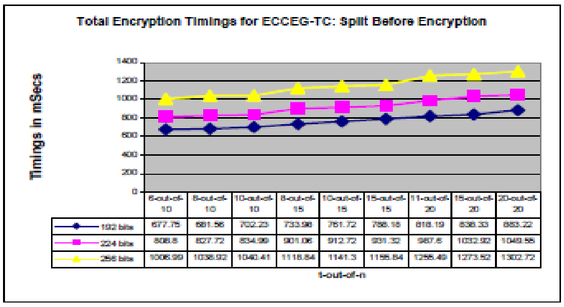

Fig. 4 Total Encryption Timings for ECCEG-TC

Fig. 5 shows that the share generation timings increase with increase in key size or with *n* or *t*. Share generation timings are very small compared to the encryption timings.

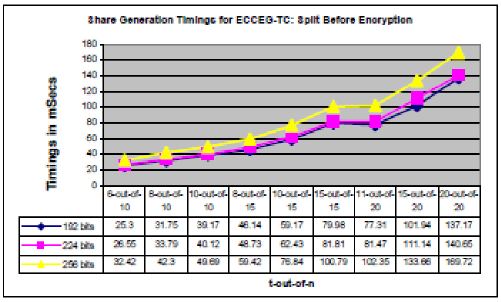

Fig. 5 Share Generation Timings for ECCEG-TC

Combination time is the time required to combine *t* partial messages using Shamir's Lagrange interpolation method to retrieve original message. From Fig. 6, the total decryption and combination timings increase gradually with increase in *t* for constant key size and *n*. This increase is due to time required to decrypt and combine additional partial messages as *t* is increased. Increase in the key size results in proportional increase in the decryption timings irrespective of *n* and *t*.

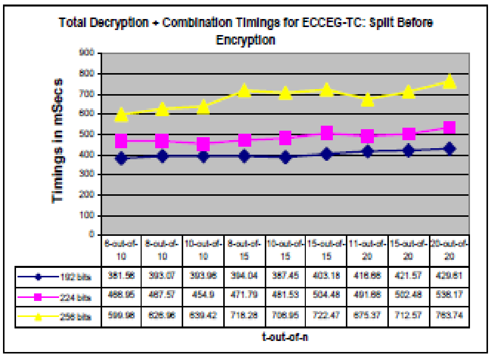

Fig. 6 Decryption and Combination Timings for ECCEG-TC

Number of point addition of ECCEG-TC increases with *n* resulting into proportionate increase in addition timing in encryption and decryption as seen in Fig. 4 and Fig. 6. The time required converting message to point and vice-versa is significantly small compared to encryption and share generation time and hence not shown separately. In ECCEG-TC, the Lagrange is carried over prime field *p*, hence the success rate is 100% as all the partial messages are recovered without any issue of inverse calculation.

V. Conclusion

An improved ILP formulation to solve the clustering trouble in MANETs. The future model offered the utilize of a Star-Ring backbone. In addition, the planned formulation incorporated the ability to enforce coverage constraints to ensure that only connections that are within the physical limitations of the node are established. Applications of MANETs are on rise and hence it is necessary to provide security to this vulnerable wireless networks. And by further exploring and implementing ECC ELgamal threshold cryptography algorithms, its shown that secure MANETs are feasible.

References

[1] S. Chinara and S. Rath, "Energy efficient mobility adaptive distributed clustering algorithm for mobile ad hoc network," in *Proc. Int. Conf. Adv. Comput. Commun.*, 2008, pp. 265–272.

[2] A. Schrijver, *Theory of Linear and Integer Programming*.New York, NY, USA: Wiley, 1999.

[3] F. Aloul, A. Ramani, I. Markov, and K. Sakallah, "Generic ILP versus specialized 0-1 ILP: An update," in *Proc. Int. Conf. Comput.-Aided Design*, 2002, pp. 450–457.

[4] D. Chai and A. Kuehlmann, "A fast pseudo-

[5] Boolean constraint solver," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 24, no. 3, pp.305–317, Mar. 2005.

[6] A. Sagahyroon, F. Aloul, and A. Sudnitson, "Using SAT-based tech-niques in low power state assignment," *J. Circuits, Syst., Comput*, vol. 20, no. 8, pp. 1605–1618, 2011.

[7] Yufang Huang, "Algorihtm for elliptic curve diffie-Hellman key exchange based on DNA title self assembly In Proceedings of 46th IEEE Theories and Applications,pp.31-36, 2008.

[8] A. M. Fiskiran and R. B. Lee. "Workload characterization of elliptic curve cryptography and other network security algorithms for constrained environments". IEEE International Workshop on WWC-5, 2009.

[9] K. Lauter, "The advantages of Elliptic Curve Cryptography For Wireless Security", IEEE Wireless Communications, vol. 11, no. 1, Feb. 2004, pp. 62-67.

[10] Y. Desmedt and Y. Frankel, "Threshold cryptosystems", in Advances in Cryptology - Crypto '89, Proceedings, Lecture Notes in Computer Science 435, G. Brassard, Ed., Santa Barbara: Springer-Verlag,1990, pp. 307-315.