DISTRIBUTED SECURE DATA AGGREGATION USING GENETIC ALGORITHM FOR MARITIME NETWORKS

Madhangi S. and Sivasundarapandian S.
Department of Electronics and Telecommunication Engineering, Sathyabama University, Chennai, India
E-Mail: madhangi1984@gmail.com

ABSTRACT

Ad-Hoc on Demand Networks is distributed open networks that establish communication on request with a minimal routing overhead. Data aggregation is alone par tedious due to its random scattered deployment. Mobile sinks, security threats, key sharing delay, etc. also influence seamless transmission between nodes. Currently existing works depend on the behavior of the nodes, by appropriately determining a gateway-like node to transmit its data and other information. The joint data aggregation and routing technique, initiated from the source recommends the collection path for each source and mobile sinks. It ensures minimum data loss and less communication disruption. The proposed system use HEC algorithm which provides low overhead in key distribution, encryption and decryption deduction when compared to the previous approaches. The joint aggregation integrating mobile sink navigation and secure hashing techniques, improves the performance of a network in terms of throughput, drop, security factor and encryption delay. Maritime tactical network requires high performance and security are one of the mainly used areas of MANET. Maritime tactical network are composed of mobile nodes (submarine, ship, aircraft etc.) and static nodes (shore stations), which can only couple with each other through radio electromagnetic spectrum.

Keywords: MTN (Maritime Tactical Network), Genetic Algorithms (GA), Ad-Hoc, Mobile Ad-Hoc Networks (MANET), HEC.

1. INTRODUCTION

A mobile ad hoc network (MANET), sometimes called as a mobile mesh network, is a self- directing network of mobile devices connected by wireless links. That is, a MANET is a group of communication nodes that wish to communicate with each other, but has no firm setup and no prearranged topology of wireless links. Each node in a MANET is free to move autonomously in any direction, and it will change their links to other devices frequently. Individual nodes are authoritative for dynamically finding out other nodes that they can directly communicate with. Due to the limitation of signal transmission range in each individual node, not all nodes can openly communicate with each other. Every node must forward traffic unrelated to its own use, and therefore be a router. Due to nodal mobility, the network topology may change expeditiously and fluctuating over time. The network is decentralized, where network organization and message delivery must be executed by the nodes alone. Message routing is a complication in a decentralize environment where the topology fluctuate. The primary challenge in building a MANET is preparing each device to continuously maintain the information needed to properly route traffic. Therefore, nodes are needed to relay packets on behalf of other nodes in order to deliver data across the network. An important feature of ad hoc networks is the changes in connectivity and link characteristics are introduced because of node mobility and power control practices.

A. Routing protocols in MANET

The primary aim of routing protocols in ad-hoc network is to establish minimum path (min hops) between source and destination with lesser overhead and lesser bandwidth use so the packets are transmitted in a timely manner. In mobile ad-hoc networks (MANETs) routing protocols are broadly categorized into Reactive (on demand) ,Proactive and Hybrid protocols. Routing protocols in Mobile ad-hoc networks are used to discover routing path between all the nodes. No access points for connecting each node to other node in network. Basically the given protocols are divided into three categories: The comparison among these protocols is described. These comparisons was based on various parameters, time period analysis, number of input as well as data sending rate for sending particular data for packet delivery ratio (PDR), end to end delay

Ad-Hoc, on demand distance vector routing protocol is a flat routing protocol it doesn't need any central authoritative system to handle the routing procedure. AODV have a tendency to to reduce the control traffic messages overhead at the cost of increased latency in finding new routes. The AODV has strong advantage in having less overhead over simple protocols which needs to keep the entire route from the source host to the destination host in their messages. So the RREQ and RREP communications which are answerable for the route discovery, do not increment significantly the overhead from these control messages. AODV reacts almost quickly to the topological changes in the network and updating only the hosts that may be affected by the modification, using the RRER message. The Hello messages, which are answerable for the route maintenance, are also limited or unavailable so that they do not create unnecessary overhead in the network. The AODV protocol is a loop free and stay away from the counting to infinity problem, which were common to the classical distance vector routing protocols.

B. Maritime Tactical Networks: Issues and challenges

Maritime tactical based network developed to promote the effective and efficient sharing of information within the maritime tactical environment [8]. MANET is the right solution to enable highly mobile, highly reactive and quickly deployable maritime tactical networks. However, when considering the application of MANETs to the tactical space, it is necessary to consider the type of platform deployed, their war fighting capabilities and communication needs [11]. Characteristics of these platforms have a significant effect on the design of the required solution. The term “MTN” used in the context of this document describes generic “networking at sea” capabilities and not a specific network. In such environment, there may be various surface ships, under water vehicles, command and control naval platform that may be fixed or mobile. Environment is extremely harsh. A fleet of ships ranging from small boats to aircraft carriers may inhabit the battle space, introducing a different degree of mobility. In addition, due to poor environmental conditions, range of radio frequencies may be pretty low and the connectivity may be irregular with widely ranging communication gaps between seconds to days.

As illustrated below in Fig-I, MTN comprises one or more Autonomous System (AS). An AS can be a collection of distributed networks such as mobile units at sea, airborne units, network operation centre (NOC) at shore or at sea. Radio Frequency (RF) is the communication medium between these units. An MTN is based on the following principles:

a) An IP based network is the most efficient and effective method for transferring planning information within a force.

b) Information transfer will take place in a Secret-High network.

c) Connections into/from other networks of a different security domain will be via approved border protection devices and

d) Ship-to-ship and ship-shore information transfers will be via a variety of strategic and tactical communication systems.

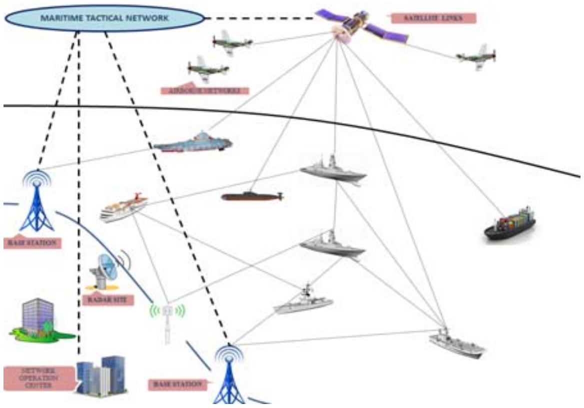

Figure-1. (Maritime Tactical Network).

2. RELATED WORK

In this section we will review the associated works of various routing and security method

Avanzi M [4] has proved that HECC over prime field is satisfactory enough when compared with Elliptic Curve, especially when large point groups are desired.

Fan and Gong [5] also proved that HECC provides greater efficiency than either integer factorization systems or discrete logarithm systems, in terms of computational overheads, key sizes, and bandwidth.

Deng Jian-zhi [6] illustrate that design of HECC based Digital signature which will solve the problem by checking the integrity of the file and signature ID, and it specifically right for the internet operation which need identity validate. It also grants the hardware module for HEC-DSA signature and validates using the simulator Quartus II 6.0.

S. Baktir [7] launches the implementation of HECC over an extension field of odd characteristic on an embedded processor and proves that implementation of genus-2 HECC over GF (281) on 32-bit ARM7TDMI processor provides an improvement of approximately 57% compared with other cryptographic algorithm. It also supplies the software employment of HECC over OTF using Microsoft’s Visual C++ Compiler 6.0 and Developer Studio 6 for writing the program for Compilation and debugging the field multiplication, field inversion and group addition and doubling.

3. THE PROBLEM IDENTIFIED

AODV [3] is totally based on distance vector routing procedure in MANETs. When security tool is applied to it, the performance of the whole network degrades. So the problem solved here is to incept security in such a different manner that the performance degradation is as low as possible.

Here the defined problems are:

1) The whole process is time consuming.

2) If given nodes or particular links fails then error message is sent back to the source this will activate the source nodes to resend the data back to destination and this will take too much time to perform the procedure again.

3) As same packet is send again and again, Traffic congestion increases.

4) Due to resending of same packet will cause other nodes in network waited to resend data, the overall effect of traffic congestion will pay impact on the throughput/performance of AODV system.

The security of AODV will be based on one-way hash, two-way hash and digital signature. All this security procedure consists of several steps. It required many functions which are inbuilt. Before sending and receiving the packet, this general Process needs to be proceeding. Now if that nodes or links fails, so all the inbuilt functions needs to be conducted again to same packet.

4. PROPOSED WORK

An MTN comprises one or more AS. An AS is a group of networks, or more accurately, the routers connecting those networks that are under the same administrative authority and that share a common routing strategy. An AS has a single 'interior' routing protocol and policy, and is also sometimes referred to as a routing domain. Interior routing information is shared among routers within the AS, but not with outside the AS systems. However, an AS may announce its internal networks to other AS that it is linked to. Each links have different resource metric for example available resources at the connecting links. Routes between the nodes are defined on the basis of number of resources like bandwidth, cost, and delay e.tc. We assume that the network topology is dynamic and the change in topology happens and updated by the deployed routing protocol only when the neighbour node changes its position. When the node finds the change in topology it updates its information and GA will restart its operation. The MTN provides a scalable, flexible, interoperable architecture that support information sharing within a maritime force. The MTN improves the richness and reach of planning and coordination information across the span of maritime operations.

Genetic algorithms (GA) are an evolutionary optimisation approach which is an alternative to traditional improvisation methods [9]. GA are most applicable for compound non-linear models where location of the global optimum is a difficult task. Genetic algorithms are a probabilistic search approach which is founded on the ideas of evolutionary change processes. The GA method is based on the Darwinian principle of survival of the fittest. An early population is made comprising a predefined number of individuals (or solutions), each represented by a genetic string (incorporating the variable data). Each distinct has an associated fitness amount, typically representative of an objective value. The concept that fittest (or best) individuals in a population will produce fitter offspring is then implemented in order to reproduce the subsequent population. Individuals are selected for reproduction (or crossover) at respective generation, with a suitable mutation factor to arbitrarily modify the genes of an individual, in order to develop new population. The outcome is another set of individuals based on the original subjects leading to subsequent populations with better (min. or max.) individual fitness. So, the algorithm recognizes the individuals with the optimising fitness values, and individuals with lower fitness will obviously get discarded from the population. The flow graph of GA is illustrated in Figure-2.

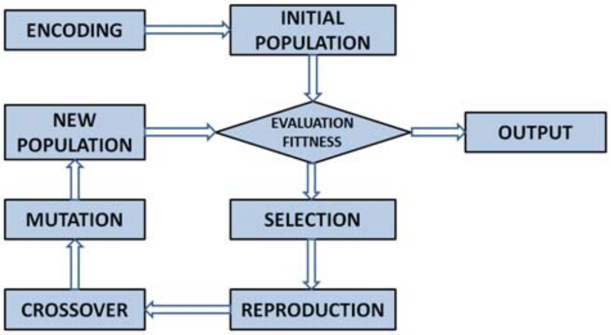

Figure-2.

Leakage of unauthorized information and penetration by unauthorized users are inherent threats in networks and may result in compromises to the confidentiality, integrity or obtainability of either the system or the information it contains. These risks are summarized below.

i. Confidentiality – Assurance that information is not disclosed to unauthorized people, processes, or devices.

ii. Integrity – Quality of an IS reflecting the logical correctness and reliability of the Operating system; the logical wholeness of the hardware and software implementing the defences mechanisms; and the consistency of the data structures and occurrence of the stored data.

iii. Availability – Timely, reliable access to data and information services for authorized users.

Cryptography is the art of science which is used to encrypt and decrypt the data for secure communication mathematically. It deliver facility to the user to transfer data securely without degrade the performance of the systems. Public key cryptography is one of the cryptographic techniques which consist of pair of keys known as private and public key. Public key is used to encrypt the data and private is used to decrypt the data. Hyperelliptic curve cryptography is the fast public key cryptographic technique with high efficiency and security [1, 2]. In 1988, Neal Koblitz suggested a new higher genus curve for cryptographic purpose known as Hyperelliptic Curve Cryptosystem. HECC has more benefit such as shorter key size, less computational overhead, high security, needs less memory space and consume less power. These features makes easy to implement HECC both in hardware and software. Since HECC has enormous feature for providing security and high efficiency for engineering application.

Genus curve decide the processing time of the Hyperelliptic Curve Cryptosystem such as key generation, encryption and decryption process. Values of g decides the polynomial of curve E like g = 2, 3, 4. Polynomial selected for genus 2, 3, 4, 5 and 6 over prime field.

5. ALGORITHM FLOW

The algorithm flow of proposed work Hyperelliptic curves are a class of algebraic curves. They can be seen as generalizations of elliptic curves. We differentiate them based on the genus of the curve. For all genus, $g \geq$ one we have hyper elliptic curves.

Let k be a field and K be the algebraic closure of k. A hyper elliptic curve C of genus g over k is defined by an equation of the form.

$$C : y2 + h(x)y = f(x) \text{ in } k[x] \qquad (1)$$
$$\text{Deg } (f) = 2g + 1; \text{ deg } (h) < g;$$

Where, f is monic and genus (g) = (deg (f)-1)=2.

- h(x) ϵ k[x] is a polynomial of degree atmost g and
- f(x) is a monic polynomial of degree 2g+1
- Deg (f) = 2g + 1; deg (h) < g;

Definition (finite points)

Let L be an extension field of k. The set of L - rational points on C are denoted C(L) is the set of points P = (x; y) ϵ L * L which satisfy the equation (1) of curve C. The points in the C are finite points.

Jacobian of hyper elliptic curve

The Jacobian of the curve C is the quotient group J =Do/P, where D is the set of divisors of degree zero and P is the set of divisors of rational functions. The equivalence classes of the Jacobian are represented by a unique reduced divisor (which is represented using Mumford representation) upon which we perform the group law.

Mumford representation

Let "g" be the genus of a hyper elliptic curve
C : y2 +h(x)y = f(x).

Each nontrivial divisor class over the field K can be represented via Mumford representation (u(x); v(x)), where u(x) and v(x), u, v 2 K[x], are unique pair of polynomials satisfying the constraints of

- u is monic;
- deg v < deg u <= g;
- u $|v^2 + vh - f$.

Algorithm for the hyper-elliptic curve cryptosystem

The beginning for the Hyper-elliptic curve cryptosystem (HECC) is the Discrete Logarithm Problem which is described as follows:

Let Fq be a finite field with q elements. Given 2 divisors, D1 and D2 in the Jacobian, determine m €Z, such that D2 = mD1. The following section describes the proposed HECC algorithm which exploits ElGamal technique for key generation procedure, encryption and decryption process which is named as HEC-ElG Algorithm (HEC-ElGA).

Algorithm for the Public Key & Private Key Generation

Input: The public parameters to be considered are hyper-elliptic curve C, prime p and divisor D.
Output: The Public key PA and Private key K_A
Process:

- K_A ϵ N [choose a prime (K_A) at random in N]
- P_A <--- [K_A].D;[The P_A is represented using Mumford representation which is of the form (u(x); v(x))]
- Return P_A and K_A.

Message encryption using HECC algorithm

We present the methodology for encryption and decryption. The message `m' that is to be sent will be encoded as a series of points represented as (u(x); v(x)).The encoded message is referred to as Em. For the encryption and decryption process using HECC, we have used ElGamal method to design HEC-ElG Algorithm (HEC-ElGA).

The algorithm works as explained below: To encrypt and send a message to B, A does the following steps.

- Private key:K_A ϵ RN (choose k_A as a random positive prime number in N);
- *Public key*:P_A<--- K_A.D

Agreed key:Q_A<---. K_A .P_B (PB is represented as receiver's public key.)

- C_A<--- {Q_A, E_m + P_A} (C_A: (u(x); v(x)) is the Cipher Text to be sent).

Message decryption using HECC algorithm

To decrypt the Cipher Text Cm, B extracts the first coordinate 'Q' from the cipher text then multiply with its Private Key (aB) and subtract the result from the second coordinate. This can be written as follows:

$$Em + k\, P_B\text{-}\ a_B(Q_A) = E$$
$$= Em + kP_B\text{-}\ k(a_BD)$$
$$= m + kP_B\text{-}a_B(kD)$$
$$= Em + kP_B - kP_B$$
$$= Em.$$

In the above process, `A' has masked the message Em by adding kPB to it. Nobody but `A' know the value of k, so even PB is a public key, nobody can remove the mask kPB. For an attacker to delete message, attacker would have to compute k from the given D and [k]D, i.e. Q, which is assumed very hard.

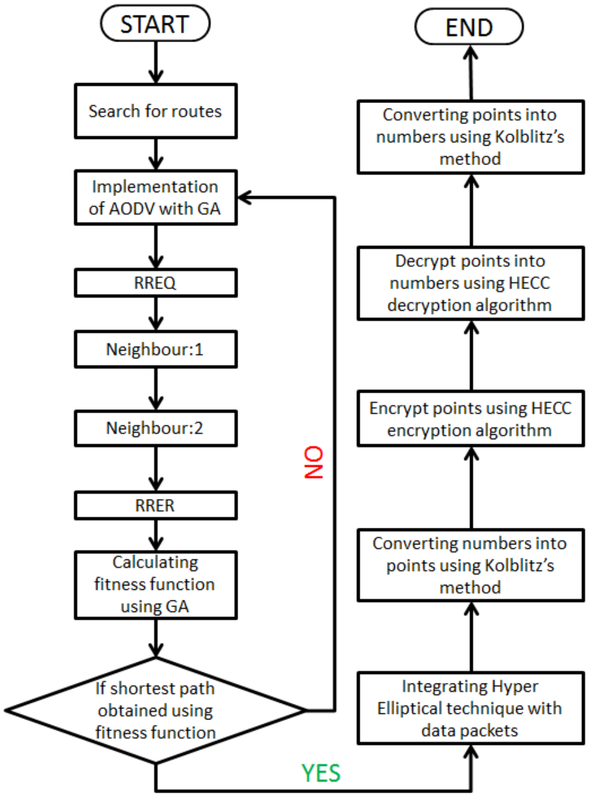
START
Search for routes
Implementation of AODV with GA
RREQ
Neighbour:1
Neighbour:2
RRER
Calculating fitness function using GA
If shortest path obtained using fitness function
NO
YES
Integrating Hyper Elliptical technique with data packets
Converting numbers into points using Kolblitz's method
Encrypt points using HECC encryption algorithm
Decrypt points into numbers using HECC decryption algorithm
Converting points into numbers using Kolblitz's method
END

Figure-3.

6. SIMULATION RESULTS

Throughput of receiving packets

This parameter will measure the successful packets received at final endpoint that are sent from the sender.

End-to-end delay

This parameter decides the delay of the sent packets between first node which is the sender and second node which is the receiver through the MANET network.

Jitter comparison ratio

In order to prevent maximum nodes in a MANET from simultaneous transmission, a given randomization of the transmission time of packets by nodes, which are known as Jitter.

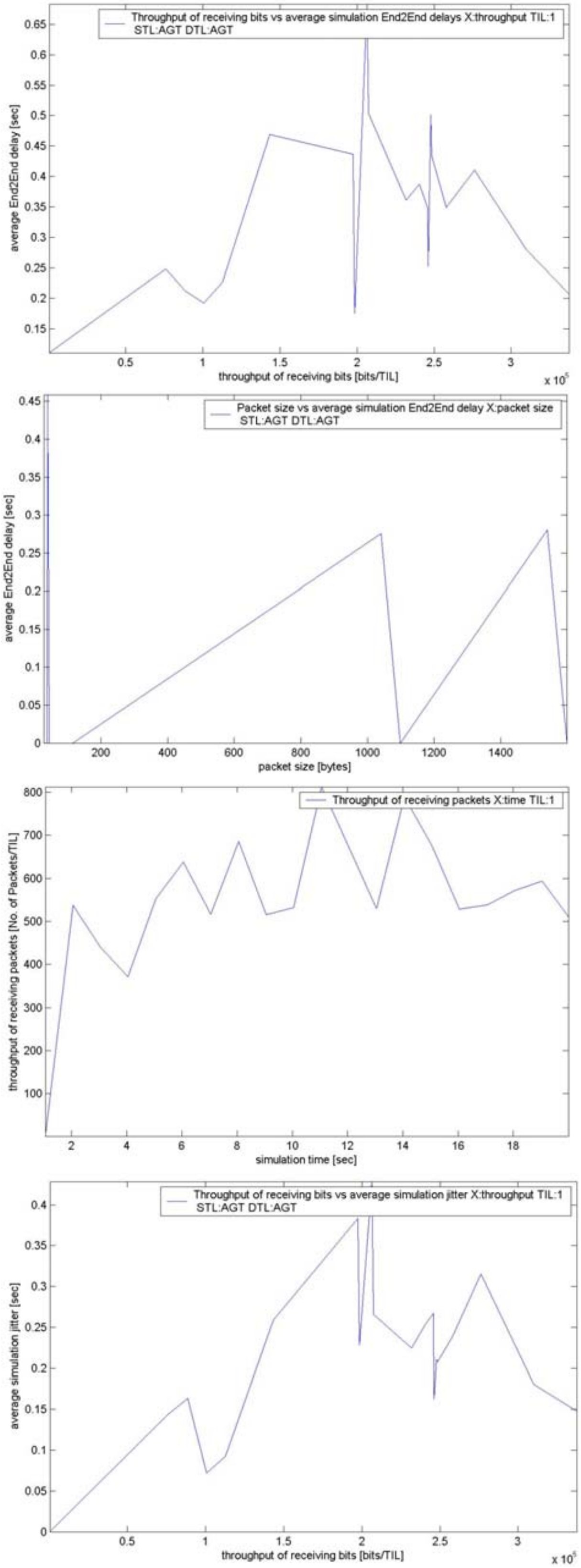

Figure-4.

7. TABULATION

The proposed work is simulated using Network simulator 2 and simulation parameter given below:

General simulation parameters	
Parameter	**Value**
MANET area	1318 X 633 sq.m.
Total number of nodes	50
Node speed	2 to 8m/s
Application	CBR/VBR
Number of generated packets	1500 packets
Size of packets	512 bytes
Simulation time	20 sec
Routing protocol	AODV
TP	TCP/UDP
Data rate	1mb
MAC	802.11
Operating frequency	2.427 e^9 Hz
Delay	10 ms

8. CONCLUSIONS

Thus this paper presents shortest path routing in Maritime tactical network using genetic algorithm with secure system. Routing security is an important issue in MANET. We need to be considering a better trade-off between greater security and network performance while designing of secure routing protocol.

We propose a method to secure AODV protocol. The proposed method uses hyper elliptical cryptography algorithm. It involves asymmetric key cryptographic operation with fast message confirmation, message authentication and in-between nodes authentication. The security is achieved by using HEC cryptography using Genus 2 curve which require less processing time for the divisor generation, key generation, decryption and encryption than genus 4, 5 and 6. The simulation result shows that recommended method reduces the time delay and network control packet overhead involved in the computation and verification of security fields. Next, the proposal, improvising security extensions and performance of AODV protocol is presented for security of the AODV routing protocol used in MANET.

REFERENCES

[1] W. Diffie and M. Hellman. 1976. “New directions in cryptography”, in the IEEE Transaction on Information Theory, Vol. 22, No. 6, November, pp. 472 - 492.

[2] W. Stallings. 2009. “Cryptography and Network Security Principals and Practices”, Pearson edition (India) Pvt.ltd, 4th Edition.

[3] C. Perkins, E. Belding-Royer and S. Das. 2003. “Ad hoc on-demand distance Vector (aodv) routing,” IETF RFC 3591.

[4] M. Avanzi. 2004. “Aspects of Hyper-Elliptic Curve over large prime fields in software implementations”, in the Springer LNCS proceedings of Cryptographic Hardware and Embedded Systems, Vol. 3156, pp. 148-162.

[5] X. Fan, and G. Gong. 2007. “Efficient Explicit Formulae for Genus 2 Hyper Elliptic Curve over Prime Fields and Their Implementations”, in the Springer LNCS proceedings of Selected Areas in Cryptography, Vol. 4876, pp. 155-172.

[6] D. Jian-zhi, C. Xiao-hui and G. Qiong. 2009. “Design of Hyper Elliptic Curve Digital Signature”, in the IEEE proceeding of International Conference on Information Technology and Computer Science, Vol. 2, July, pp. 45-47.

[7] S. Baktir, J. Pelzl, T. Wollinger, B. Sunar and C. Paar. 2004. “Optimal Tower Fields for Hyperelliptic Curve Cryptosystems”, in the IEEE transaction of Signals, Systems and Computers, Vol. 1, pp. 522-526.

[8] D. Kidston and T.Kunz. 2008. “Challenges and Opportunities Managing Maritime Networks” IEEE Communications Magazine, October.

[9] L. Davis. 1991. “Handbook of Genetic Algorithm,” Van Nostrand Reinhold, New York, USA.

[10] Fabio Garzia, Natale Tirocchi, Michele Scarpiniti and Roberto Cusani. 2012. “Optimization of Security Communication Wired Network by Means of Genetic Algorithms“, Communications and Network, Published Online in http://www.SciRP.org/journal/cn, August.

[11] L. Kant *et al.* 2008. “Network Science Based Approaches to Design and Analyze MANETS for Military. Applications,” IEEE Communication magazine, November.