International Journal of Engineering & Technology, 7 (2.7) (2018) 16-19

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper



A Secure data packet transmission in wireless sensor network using HECC algorithm and Finding malicious packet

M.Venkateswara Rao[1*], K.Raghava Rao[2]

[1] *Ph.D.Scholor, Department of Computer Science and Engineering, KLUniversity,Vijayawada, India*
[2] *Professor, Department of Computer Science and Engineering, KLUniversity,Vijayawada,India*
**Corresponding author E-mail: venkat2m2@gmail.com*

Abstract

The most important purpose of implementing to share secure knowledge in encrypted kind in network is to extend the safety of personal networks and its databases and to additionally give remotely infrastructure less secure services globally. In the current system approach ECC elliptic curve cryptography is being used to deal with the security issue in wireless sensor network. Thus the system still get a long packet transfer time, which can be further become a disadvantage while dealing with large data packet. Thus the system further and study require reducing the computation transfer time in between the packet. A proposed hyper elliptic curve mechanism for the cryptography can be used to opt out the best performance over the data packet transfer. In this scenario HECC algorithm is utilized and hence the result outcome shows the efficiency of the algorithm.

Keywords: *HECC, WSN security, security threads, Path discovery.*

1. Introduction

Wireless communication entity interlinked scenario is a process of beaming information from one point to another peak without using any physical medium or wire. A routing optimized technique Ant colony is proposed in the previous solutions. It contains various types of fixed, mobile and portable application [1]. Mobile multiple communication entity connection contentment with Wireless multiple communication entity connection Interfaces become a significant component of the computational entity where multiple communication entity interlinked scenario. A critical constraint on sensor multiple communication entity interlinked scenario is that communication connected sensor movements of multiple communication entity connection contentment gives power consumption [3]. The approach followed by the system need to enhance in terms of delivering high end performance alongside the better security over the network communication.

Military protocol architecture: the multiple and fast multiple communication entity connection and system configuration, automated-organizing and fault tolerance configuration and multiple communication entity connection properties of sensor multiple communication entity interlinked architecture make it working with the high end security requirement platform such as military application [8] , command, communication entity interlinked scenario, intelligence, computing, reconnaissance, surveillance and targeting strategies. A military based network and other DTN network help in merging the working of communication entity such as neural system and other based system such as biological, attack relevant entity solution. These help in generating better reliable communication over the provided network area[4].

2. Related Work

As we know that mobile data packets transmission in wireless sensor multiple communication entity interlinked scenario movements of multiple communication entity connection contentment for creating multiple paths from start-up point to the destination place [6] ,the current or previous protocols. The ways of disjointedness is categorized as communication entity disjoint, link disjoint & partially disjoint.

3. Ant Colony Optimization

The ants always tries to cover the shortest distance to reach their final stop, which has food in outcome.
The path from which they go throughout has a concentrations that allows them to find their food source and thus, more will be the collection of pheromone will be there with more no. of ants that passes through that path.
Rules for the shortest path finding:

1. Every system hub sends numerous revelation bundles - forward ants (F-ANT) towards the selected goal hubs of the system.

2. The random tables follow the steering at each hub keeping in mind the tip goal to select next bounces in step with the weighted chances accessible.

3. The steering table's area unit modified for alternative of the subsequent hub within the system.

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

4. At the purpose once forward subterranean insect (F-ANT) achieves the goal hub, it creates a regressive insect (B-ANT) and subsequently passes on. equally in MANETs steering, the new parcel created and sent back to the supply can proliferate through an identical manner selected by the forward subterranean insect (F-ANT).

In [13] Gustavo S described the asymmetric encryption technique in between the wireless sensor network for communication and security providing architecture. They have stated that the RSA is the most revealing and best approach among the given algorithm. Further they have also stated that the ECC and HECC approach algorithm can be further being applied on the network. They have given example of embedded sensor which works with the encryption technique over data transmission unit in between the given entity [9, 10]. According to them it can be work with physical layer and transmission of node network data can further be given in this approach. The further working with the same scenario is left by them for future work.

In this paper [11], authors propose A Mobile spontaneous Network (WSN) relies on a self-organizing and quickly deployed network. During this network all nodes are mobile and communicate with one another via wireless communications. Nodes will be part of and leave at any time and there's no mounted infrastructure. All the nodes are equal and there's no selected router nodes that will function routers for every alternative and knowledge packets are forwarded from node to node in a very multi-hop fashion. WSNs within the recent past. Ant-based routing provides promising different to traditional approaches [12]. These agents ar autonomous entities, each proactive and reactive, and have the aptitude to adapt, get together and move showing intelligence from one location to the opposite within the communication network.

ACO based routing for WSNS [2], in this paper; authors propose a Mobile impromptu network (WSN) could be a assortment of wireless mobile nodes. It dynamically forms a brief network while not victimisation any pre-existing network infrastructure or centralized administration i.e. with negligible previous coming up with [5].

Simulation Parameters

The simulation configuration used for the current analysis summarized in below table:

Table 1: Configuration files settings

Parameter	Value
Total Simulation Timing relevance parameter	3600s
World Size	4500 X 3400 m
Movement Model	Cluster Based Movement
Communication entity Buffer Size	5M
Route adapting communication Protocol	Wave router
No of Movements of multiple communication entity connection contentment	126
Interface transmit Speed	2 Mbps
Interface Transmit Coverage	10 m

The table 1, above it describes the detail discussion of simulation setup and scenario performed.

4. Related Work

The differences between the several algorithms has been find out through the related work.

DES: many attacks has been done that has made it an insecure block cipher

3DES: this version was introduced afterwards the des block cipher. Since it is a well known fact that it is slower than the des.

AES: this is introduced just to replace the des for the smooth working, also this is an advanced version of des.

Blowfish: it is also called as public domain encryption algorithm. Blowfish has a variable length key, 64-bit block cipher.

5. Proposed Algorithm

Hyper elliptic Curves Cryptography:

This algorithm use to secure the wireless network because this algorithm is use global variables. The security of hyper elliptic Curve Cryptosystem [13] depends on the distinct index downside. This downside helps to avoid the hearer from breaking of keys even each letter of the alphabet and P values area unit glorious in public. Differing types of curve got to study to know regarding public key (Q), cluster purpose (P).

Hyper egg-shaped ambit E of brand g>=1 over bound filed F is the set of band-aid (x, y) ϵ F*F to

The equation

E: y2

+ h(x) y = f(x) (1)

Where h(x) is a polynomial of amount g and h(x)ϵF(x), f(x) is a berserk polynomial of

Degree 2g+1 and h(x) ϵ F(x). The ambit E is said to be non-singular curve, if there are no pairs

(x, y) ϵ F*F. The polynomial f(x) and h(x) are called such that it has to amuse the following

Equations

2y + h(x) = 0 (2)

h'(x) y – f'(x) = 0 (3)

6. Proposed Methodology

In order to perform proper communication in between the node and data availability, the proposed methodology work perform the security approach over the communication node in wireless sensor network to perform the communication in between end to end entity. There are performed procedure applied security approaches over the node communication in these ways:

1. First of all, communication node setup, data entity, node scenario is generated along with the mobility, data packet size, packet rate etc.
2. Further be the packet transmission and size described is applied.

3. A communication entity in between the source and sink is been described to perform communication in between the nodes.
4. An HECC encryption approach over the computation is taken and parameters are computed for the communication [7].
5. Neighbour node determination and computation distance between both the nodes, start communication in between them.
6. Encryption process is applied on data packet before transmission to the neighbour node.
7. Data packet which is encrypted is send to the neighbour node and thus process to the destination direction according to path.
8. Data packet receiving and computation according to number of sending packet and receiving packet.
9. Compute parameters such as packet delivery, communication time, data packet network security using different cryptography approach.
10. Exit.

Below is the pseudo code that will explain the work of the proposed algorithm clearly.

Step1: Setup (node, data entity) along with mobility, data packet size, packet rate
Apply: Packet Transmission, size
Step2: Compute parameters
On the basis of nodes (distance)
Step3: If (neighbour node determination and computation distance found)
Start communication between them
Step4: Apply Encryption process on (data packet)
Then, send to neighbour node
Step5: Compute parameters
Exit:

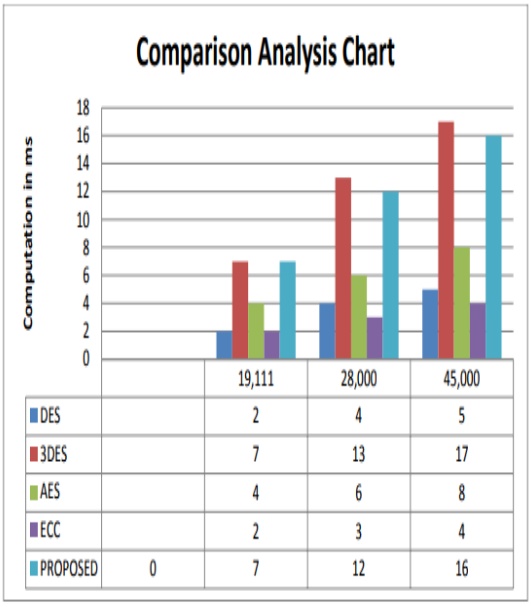
7. Result Analysis

The popular secret key algorithms including DES, 3DES, AES, Blowfish have been simulated on machines: P-4 2.4 GHz using crypto++ simulator and the results obtained from this simulator has been incorporated. These results have been compared with our Proposed Algorithm and simulation program both developed in java , and run on the same machine i.e. P-4 2.4 GHz. The comparison has been summarized in the table 2.

Table 2 explains various comparisons

Input Size (bytes)	**DES**	**3DES**	**AES**	**HECC Hybrid Approach**	**ECC Approach**
19,111	2	7	4	2	7
28,000	4	13	6	3	12
45,000	5	17	8	4	16

The above table 2 described the result analysis and obtains from different communication encryption algorithm used in environment.



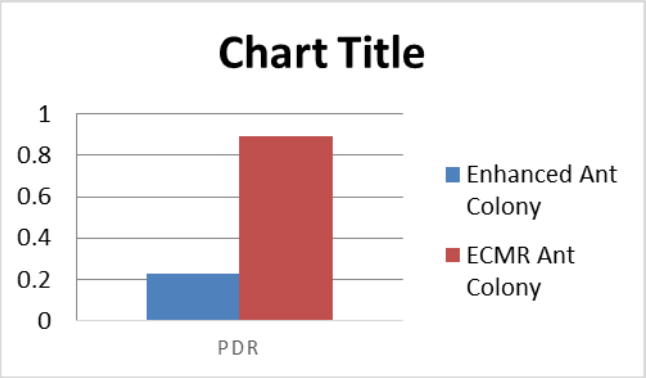
Graph 1: Encryption Performance

From the graph and table 'Proposed Algorithm' has an advantage over 3DES in terms of throughput. The results showed that 'Proposed Algorithm' 3DES algorithms.
PDR, relay and Overhead for existing and proposed technique over network.

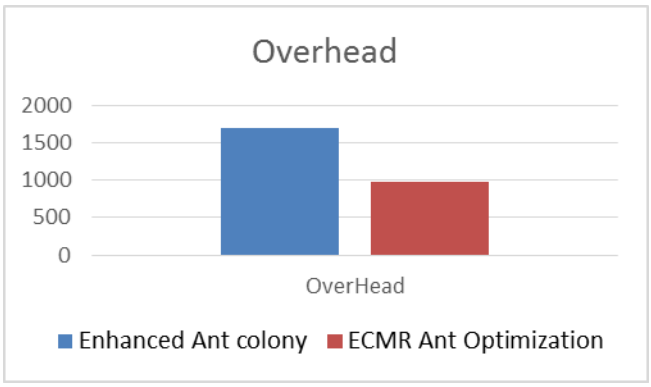
Algorithm	PDR	Relay	Overhead
Enhance Ant Colony	87.55	91.26	67.1
HECC Based Ant Color	91.21	84.50	72.76

Graphical Result Analysis:

A graphical analysis for existing and proposed technique is presented in this section



Graph 5.1: comparison of relay for Existing and Proposed technique.



Graph 5.2: Comparison PDR for existing and Proposed Technique.

As per the result observed using the proposed technique HECC Ant Optimization provides the better output and result in order to improve the life of network over MANET.
From the graph and table observe that 'Proposed Algorithm' has very efficient on high configuration machine. The results showed that 'Proposed Algorithm' has a very good performance on quad machine.

8. Conclusion

WSN is an important part of today's technology, it discuss with the various routing protocol which commit to communicate in short span of time and dedicated communication in between various scenario. Mobile adhoc network need proper security with enhancement of communication encrypted unit for secure communication. In this paper a work is performed towards the security algorithm which takes part in previous secure algorithm and thus a study is performed over packet transmission. In previous work some security algorithm is observed, but a proper routing protocol along with security is not given. Hence an advance HECC algorithm with ACO algorithm for routing is combined to provide a hybrid solution for communication as well as secure packet transmission. Our result observed shows the efficiency of proposed algorithm as best while compared with existing approach. Our further work is going to concentrate more on energy and QoS with the approach performed by us.

References

[1] XUXUN LIU," Routing Protocols Based on Ant Colony Optimization in Wireless Sensor Networks: A Survey",IEEE Access, Digital Object Identifier 10.1109/ACCESS.2017.2769663.
[2] Peng Huang,1,2Feng Lin,3 and Jiliu Zhou3, ACO-Based Routing Algorithm for Cognitive Radio Networks
[3] Alexey S. Matveev and Andrey V. SavkinMultirate Stabilization of Linear Multiple Sensor Systems
[4] Charles E. LaljerThe MITRE Corporation San Antonio, TX 78227,CHEMICAL AGENT DETECTOR
[5] Peng Huang,1,2 Feng Lin,3 and Jiliu Zhou3, ACO-Based Routing Algorithm for Cognitive Radio Networks.
[6] Rouleau, Robert and Hodgson, Ian (1981). Packet Radio. Tab Books, Blue Ridge Summit, PA. ISBN 0-8306-9628-8.
[7] Admilson R. L. Ribeiro and Edward David Moreno, Asymmetric Encryption in WirelessSensor Networks.
[8] Orly Stan, Yuval Elovici, AsafShabtai, proposed military protocol architecture.
[9] DebapriyaBasu Roy, Poulami Das, and DebdeepMukhopadhyay, ECC on Your Fingertips
[10] It is explained by the wikipedia: https://en.wikipedia.org/wiki/Unit_interval_(data_transmission).
[11] Mohammad JalilPiran1 , G. Rama Murthy2 , G. Praveen Babu3
[12] LuisCobo,AlejandroQuintero,SamuelPierreAnt-based routing.
[13] Gustavo S. Quirino, Admilson R. L. Ribeiro and Edward David Moreno, Asymmetric Encryption in Wireless Sensor Networks INTECH 2014.