International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 9 (2015) pp. 22821-22834

http://www.ripublication.com

Efficacious Data Transmission Using Adequate Energy To Avert Fake Agent Attackers

S. Lavanya
Department of CSE, Paavai Engineering College, Anna University, TamilNadu.
Mail Id: lavanyaresearch01@gmail.com
Dr. V. Murali Bhaskaran
Principal, Dhirajlal Gandhi College of Technology, AnnaUniversity, TamilNadu.

Abstract

Wireless Sensor Network generally deployed in natural environment, so large number of security is emits are there. Protect the data in WSN require approaches that will make data transmission more secure from the attackers. Data transmission can be performed based on cluster using imperialist competitive algorithm. It can partition the cluster in to sub-clusters and compete with each other until one of these cluster nodes is preferred. For efficient data transmission to exploit key selection from elliptic curve as an Aeolian group with point as fundamentals,ECAES algorithm is used. To pass up fake identities in packet can be transferred, the dissimilar approach called fake agent attackers is used which prevent the traffics and fake distinctiveness of nodes located at communication range around target area. Energy efficiency can be improved by using Adequate energy which select the most appropriate neighbor node with position closeness and substitute node is not only required to be close to the faulty node to ensure the correctness of sensing, but also have higher residual energy to guarantee further constancy. So the efficient utilization of algorithm is used to reduce dropping ratio and minimize overhead.

Keywords: WSN, Adequate energy, ECAES, fake agent attackers, Imperialist Competitive algorithm.

Introduction

Wireless Sensor Network

In wireless communications have enabled low cost, low-power, multifunctional sensor nodes for the development that are small size and short distances communication. The tiny sensor nodesare used inthe sensor networks, which consist

of sensing, data processing, and communicating components. A sensor node is a node in a wireless sensor network that is capable of performing rarefaction, sensory information for congregation and communicating with other consecutive nodes in the network. Wireless sensor Network is connected with algorithms and set of protocols for efficient communication to connecting the nodes. The energy efficiency provided adequate energy that select the neighbor node also close to faulty node and stable residual energy for reducing the dropping packets

The problem consists of monitoring a set of targets in a designated geographical area to a satisfactory level for packet dropping it is nothing but a bad node drops all or some of the packets that are supposed to be forwarded. It can also drop the data generated by itself for some malicious purpose such as blaming innocent nodes. It may also modify the data it generates to protect itself from being identified or to accuse other nodes. A detection technique is to detect unauthorized or unusual behavior in a network, Intrusion Detection System and node monitoring techniques are used for detection. The attacker knows the minimum misbehavior threshold and if they can manipulate the packet dropping rate, it becomes difficult to detect the misbehaving node. The Intrusion is an unauthorized (unwanted) activity in a network that is either achieved passively used information gathering, eavesdropping or actively used harmful packet forwarding, packet dropping, and hole attacks. The packet dropping and modification is a main problem to overcome that used another attack to prevent the loss in packet. The schemes effectively detecting the dropping packets, low communication and overheads of energy, being compatible problem in the dropping or loss among packet through mitigate the attacks. Within a certain number of hops the packet dropping is used filter modified messages en-route. These countermeasures can tolerate or mitigate the modification attacks and packet dropping, but the intruders are still there and can continue attacking the network without being caught. The node categorization algorithm to identify nodes that are packet droppers for sure, suspicious packet dropper's problem in traffic rate and static only.

To overcome these problem use fake agent attackers, a huge number of identities are forged and fake identities are created by the malicious nodes in the network to avoid the fake distinctiveness. To divide the cluster into sub cluster by using Imperialist Competitive Algorithm(ICA) is one of the most powerful algorithms; it has been used extensively to solve different kinds of optimization problems. In this ECAEC is modern technique for encoding and decoding purpose. The various energy sources having different methodsare more sufficient, in adequate energy to improving the energy efficiency that to selected the nearby node with hurler position. In Substitute node not only required be close with faulty node but also sensing accuracy is ensure, after select the cluster header use ECAES Algorithm to select a key, to identify the fake agent attackers by using this algorithm.

Architecture Diagram for Proposed System:

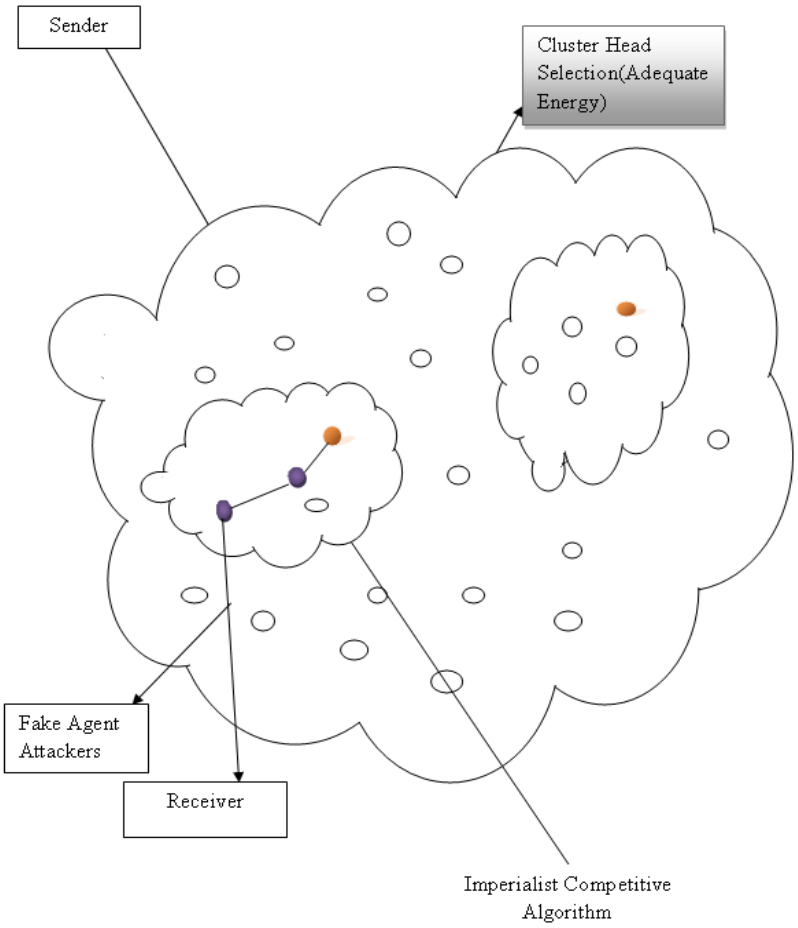


Figure 1: Architecture Diagram

The sender selects the node by using the ECAES Algorithm, the cluster can be divided into sub cluster and the sub cluster will select the cluster head. After select the cluster header use ECAES Algorithm to select a key, to identify the fake agent attackers by using this algorithm. The adequate energy can analysis the energy efficiency to select the closer position node, after select the node by using Imperialist Competitive Algorithm to find the shortest path and to send the data to the receiver**.**

Literature Survey

In paper [1] packet drop attack detection techniques in wireless ad hoc networks have gained lots of attention due to their ease and low cost of deployment of ad hoc networks has great importance in numerous military and applications of civilian. The lack of centralized management of these networks makes them vulnerable to a number of security attacks. The attacks are attack of packet drop, which a compromised node

drops packets maliciously. To detect the packet drop attack in wireless ad hoc networks, the packet drop attack detection techniques their ability of attack under different attack strategies (partial and or Attacks of cooperate),the computational and communication overheads andenvironments caused in the detectionprocess. The malicious packet dropping in wireless ad hoc networks considering the two common routing protocols AODV and OLSR. The malicious packet dropping detection techniques proposed to assess their effectiveness and limitations. The watch dog though produces less computational and Communication overhead is susceptible under partial and cooperate attacks. The SCM produces Average computational and communication overheads as it detects different kinds of attacks in Mobile environments. The monitoring agent produces high overheads in detecting different types of attacks and is susceptible in mobile environments. The sequence number technique as Well produces high overheads and is susceptible in mobile environments and does not detect types of all attacks. Depending on the anticipated attack strategy, network environment (mobile or stationary) and the Processing power of the nodes to be used in a given wireless ad hoc network the choice of a Malicious packet dropping technique. The Malicious packet dropping detection technique that effectively detects the attacks based on the packet dropping attack in a Wireless Sensor Network.

In paper [2], Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks Link error and malicious packet dropping are two sources for packet losses in multi-hop wireless ad hoc network.The link errors createa sequence of packet losses or the link errorscombined effect and malicious drop provides the losses in the network. In malicious nodes that are part of the route exploits their knowledge of the communication context to selectively the insider attack drop a small amount of packets critical to the performance of network. Therate of packet dropping is comparable to the channelerror rate;predictable algorithms that are based on detecting the packet loss rate cannot achieve accuracy of satisfactory detection. Theyimproved the detection accuracy to use the correlations between missing packets. Ensure truthful calculation of these interrelations, they developed a homomorphism linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes. It is privacy preserving,proof of collusionand low communication incurs andoverheads of storage. It reduce the computation overhead of the baselinescheme, amechanismof packet-block basedis also proposed, which allow one to trade detection accuracy for lowercomplexity of computation. They verified that the proposed mechanisms achieve significantly better detection accuracy than conventional methods such as a maximum-likelihood based detection during wide-ranging simulations.

In paper [3], CTCP: A cross-layer information based TCP for MANET Traditional TCP cannot detect link contention losses and route failure losses which occur in MANET and considers every packet loss as blocking. The degradation of TCP performance in this effort of research, they modified the operations of TCP to adapt to network states. The cross-layer notifications are used for adapting the congestion window and achieving better performance. The Cross-layer information based Transmission Control Protocol (CTCP) which consists of fourstates of network. Slow

down state to recover fromlosses of contention, Cautionary state to deal with route failures, packed state to handle network congestion and Normal state to be compatible with traditional TCP. Decelerate state makes TCP slow down if the packet loss is believed to be due to contention rather than congestion. Condemnatory state can suspend the TCP variables and after route reestablishment resumes withconservativevalues. Calls of Congestion statecongestion control when network is actually congested and normal state works as standard TCP. By putting CTCP into four states thecross-layer informationbased messages give an explicit notification to CTCP to react according to the contention, congestion or route failure.Decelerate state to make progress fromlosses of contention, Cautionary state to deal with route failures and Congested state to handle network congestion and Normal state to be compatible with TCP.

In paper [4], Performance Comparison of Energy Efficient Protocols for Wireless Sensor Networks is often partitioned into clusters, cluster head(gateway) can managethe each cluster. In wireless sensor networks,the medium access control (MAC) is an empowering technology. MAC protocols control how sensors access a shared radio channel to communicate with neighbors in small area coverage. It classifies traditional (IEEE 802.11) and a power efficient gathering protocol and existing MAC protocols, called as PEGASIS, for a sensor network as examples of MAC protocol designed specially. SENSOR MAC sets the radio to sleep during transmissions of other nodes unlike PEGASIS which involves non sleeping cycles. The performance impact of sleep in a Sensor-MAC protocol and non-sleeping based IEEE 802.11 by evaluating PEGASIS,that makes use of PEGASIS protocol exhibits higher throughput as compared to the scenario that uses SENSOR MAC protocol in small network area. In SENSOR MAC protocol the nodes undergo periodic sleep states to conserve the energy, the node is in sleep state then the other node has to wait for the node to enter listen mode so that data can be transferred. This waiting time reduces the throughput of the network, it is observed that the throughput increases of nodes increases attains a highest value and then it starts decreasing as the numbers of nodes in the WSN. The performance impacts of latency and energy consumption under varying duty cycles and for different arrival ratesof packet, etc.

In paper [5], Combating Congestion Problem in Wireless Sensor Network using Combined Dominating Set Technique consists of small nodes with sensing,e capability ofcommunication and computation. These sensor nodes are small tiny devices, the data can be transferred from one node to another by gathering a sensor nodes. Due to failure in these sensor nodes packet may get dropped in the network due to which throughput get decreased and retransmission of data packet from sender node to receiver node leads to energy consumption which in return cause delay in data packet delivery at sender end. Main categories arelocation andhierarchical based and data centric. Every algorithm or technique have common objective to less delay, less energy consumption and better lifetime of network. These various techniques and parameters, they introduced a new technique named Combined Dominating Set (CDS). This technique is to avoid congestion and to increase link stability. on the basis of delay, energy consumption and the network lifetime, the various parameters which got affected by the occurrence of congestion in the network. In Mint route

technique data packet get forwarded to another node without observing demerits of that selection of route, probability of congestion occurrence increases. TADR identifies alternative routes with multiple paths where sensor nodes are either idle or less overloaded. To alleviate congestion in the network a new technique called TADR Combined Dominating Set (TADR-CDS). They minimized delay and energy consumption with this technique.

In paper [6], Congestion Control in Wireless Sensor Networks for defense, health monitoring and temperature monitoring, Congestion occurs in the sensor network because of limited resources such as sensor nodelow processing power. Sensor nodes are battery powered, congestion in the sensor network results in waste of energy of sensor nodes and the network can be involved in the congestion control process. Fairness aware congestion control (FACC) scheme, nodes are categorized according to their position from base station node. Nodes which are near to sink are called as near-sink nodes(nodes of near Base station). Nodes which are far away from sink are called as near-source node. Near-sink node according to state of per flow allocate rate to each passing flow, the change of flow, there is lightweight probabilistic dropping algorithm use. This algorithm is used as per queue occupancy and strike frequency. In this method, compare to near source node near sink nodes has to transfer more traffic. Next to sink node do not need to maintain per flow state and it just generate warning message after drop of a packet.

In paper [7], Quality of Service Enhancement of Wireless Sensor Network Using Symmetric Key Cryptographic Schemes is a combination of spatially distributed independent nodes deployed in dense environment, communicating wirelessly over limited bandwidth and frequency. Security and QOS is the network due to its wireless communication nature and constraints like low computation capability, less memory, bounded energy resources, susceptibility to physical capture or damages and the use of insecure wireless communication channels. Along with the QoS these constraints make security, a challenge in wireless sensor network. The cryptographic schemes increases the level of security and make it secure against critical attacks but also has a significant impact on the QoS of wireless sensor network. The different cryptographic schemes based on asymmetric key and symmetric key cryptography are evaluated. Thecryptography schemes of symmetric key require less time for processing, less power and also require less storage space as compared tocryptographic schemes of asymmetric key, results in less impact on the QoS of wireless sensor network. The effective cryptographic schemes selection depends on the processing capability of the sensor nodes characterized by the constraints on energy, computation capability, less memory and communication bandwidth.

In paper [8], in wireless sensor networks Path Reconstruction in Dynamic Wireless SensorNetworksUsing Compressive Sensing a compressive sensing based approachfor path reconstruction. An arbitrary routingpath can be represented by a path vector in the space by viewingthe whole network as arepresentation space of path. Since pathlength is usually much smaller than thesize of network, the pathvectors are sparse, i.e., the majority of essentials are zeros. The path vector (andthus the represented path) can be recovered from a small amountof packets using compressive sensing technique by encodingsparse path representation into packets.

CSPR formalizesthe sparse path representation and enables accurate and reconstruction of efficientper-packet path. CSPR is secure to network dynamics and loss links due to its distinct designthey evaluate CSPR in both test bed-based experiments and simulations of large-scale trace-driven. The approachesof state-of-the-art, CSPR is essentially insensitive to network dynamics andlinks of loss. Wide-ranging evaluations through both testbed-basedexperiments and trace-driven simulations show that CSPR outperforms the state-of-the-art approaches in various network settings.

In paper [9], in wireless sensor networks Multi-hop Route Discovery Using Opportunistic Routing for Wireless Sensor Networks a compressive sensing based approach for path reconstruction. In the space, by viewing the whole network as a representation space of path, the path of arbitrary routing can be represented by a path vector. Sincethe path length is usually much smaller than the size of network, the path vectors are sparse that isthe elementsmajority are zeros. The path vector (and thus the represented path) can be recovered from a small amount of packets using compressive sense techniqueby encoding sparse path representation into packets. CSPR formalizes the sparse path representation and enables accurate andreconstruction ofefficient per-packet path. CSPR is invulnerable to network dynamics and loss links due to its distinct design. CSPR in both test bed-based experiments and large-scale trace-driven, achieves high path recovery accuracy and the art approachesstate in various network settings.

In paper [10], Route to Avoid Congestion in Wireless Sensor Networks used the limited transmission range of sensor nodes. Opportunistic Routing is a multi-hop routing for wireless sensor networks. The neighbors of sender node overhear the transmission and form multiple hops from source to the destination for transfer of information. The neighbor nodes set participating in the routing are included in the forwarder list in the priority order. The node with highest priority is allowed to forward the packet it hears. A new protocol by Energy Efficient Selective Opportunistic Routing (EESOR) that reduces the size of forwarder list by applying a condition that the forwarding node is nearer to the end node. The path followed by acknowledgment packet follows opportunistic routing, assuretransmissionreliability and energy balancing. EESOR protocol performs better than existing Energy Efficient Opportunistic Routing (EEOR) protocol with respect to parameters End-to-End Delay, Throughput, Routing Overhead and Network Lifetime.

Methodologies In Proposed System

ECAES Algorithm

Encryption and Decryption can be done by using Elliptic Curve Authenticated Encryption Scheme (ECAES) or simply called elliptic curve Encryption Scheme, ECAES algorithm is a deviation of public-key encryption. ECAES encryption for certain data integrity and authentication, exploit the session keys (symmetric keys) for encryption of data. Session keys are interchanged using ECAES encryption. To authenticate the nodes and generate session keys between the nodes and the sink, in

between the nodes need to communicate. Public key Encryption is support for semantic security. For selecting the random numbers, the Elliptic Curve Authenticated Encryption Scheme to encrypt the message, forcluster divide into two sub clusters by using ICA and form a sub cluster to select the cluster head that select the key by using ECAES Algorithm. To decrypt a cipher text to perform a key validation on verifies, check and compute the Keys.

It is an efficient scheme which provides semantic security against towards allowed using algorithm. The scheme of the security is based on the ECAES algorithm. Two IES standardized are Discrete Logarithm Integrated Encryption Scheme (DLIES) and Elliptic Curve Integrated Encryption Scheme (ECIES), which is also known as the Elliptic Curve Augmented Encryption Scheme or simply the Elliptic Curve Encryption Scheme. Alice can encrypt and bob can decrypt the message by using the efficient ECAES algorithm the optional sharing information also available to share the message.

Public key possesses not only confidentiality but also characteristics like enforceability and non repudiation. For Heterogeneous Sensor Networks, the scheme of an efficient key management based on public key elliptic curves cryptography scheme, it is optimized for cluster sensor networks and is efficient in terms of difficulty, computation ,number of message exchange andrequirements of storage with optimized security benefits for clustered surroundings. The key management possesses not only confidentiality but also characteristics likenon repudiation and enforceability. The ECAES Algorithm have efficient key management scheme for exchange message to compute a different measurement of security. Thestrengths cryptographic of a cipher algorithm may depend according to the definition only on the used key that is kept secret.

This means a potential attacker may know the algorithm itself, the plain text, the encrypted text and even the length of the key. The attacker can test different numbers in order to disclose the key, such an attempt is called brute force attack and the attacker needs to test 2n number in the worst case to get a key of length n. The average number of attempts is $2n-1$. For running the cipher algorithm, the attacker gets physical access to device, the attacker can record not only the input and output values of the completed cryptographic operation but also intermediate values of the cryptographic operation that provide additional information and by that simplify the determination of the key.

Thecryptosystems of symmetric key are preferred over public key systems due to the following factors:

1. Ease of computation
2. Smaller key length providing the same amount of security as compared to a larger key in Public key systems.

Alice has the domain parameters D = (q, FR, a, b, G, n, h) and public key S. Bob have the domain parameters D. Public key of the Bob is S_B and private key is D_B. The mechanism ofECAES is as follows.

Alice executes the following stepsA does the following

Step 1: Selects a random integer r in [1, n – 1]

Step 2: Computes R = rG

Step 3: Computes $K = hrS_B = (K_x, K_y)$, verify that $K \neq \boldsymbol{O}$

Step 4: Computes keys $k_1||k_2 = KDF(K_x)$ where KDF is a function of key derivation, which derives cryptographic keys from a shared secret

Step 5: Computes $c = ENC_{k1}(m)$ where m is the message to be sent and ENC a symmetric encryption algorithm

Step 6: Compute $t = MAC_{k2}(c)$ where MAC is message authentication code

Step 7: Sends (R, c, t) to Bob

To decrypt a cipher text, Bob performs the following steps

Step 1: Perform a partial key validation on R (check if $R \neq \boldsymbol{O}$, check if the coordinates of R are properly represented elements in F_q and check if R lies on the elliptic curve defined by a and b)

Step 2: Computes $K_B = h.d_B.R = (K_x, K_y)$, check $K \neq \boldsymbol{O}$

Step 3: Compute $k_1, k_2 = KDF(K_x)$

Step 4: Verify that $t = MAC_{k2}(c)$

Step 5: Computes $m = ENC_{K_1^{-1}}(c)$

We can see that $K = K_B$, since $K = h.r.S_B = h.r.d_B.G = h.d_B.r.G = h.d_B.R = K_B$

The primary security in ECC is the parameter n; therefore the length of ECC key is the n-bit length. The ECC security keys is much more than that of other cryptosystems for relative length. The key length of ECC key is much lesser than other cryptosystemsfor security of equivalent.

The Fig.1 given below demonstrates the Elliptic Curve Authentication Encryption Scheme

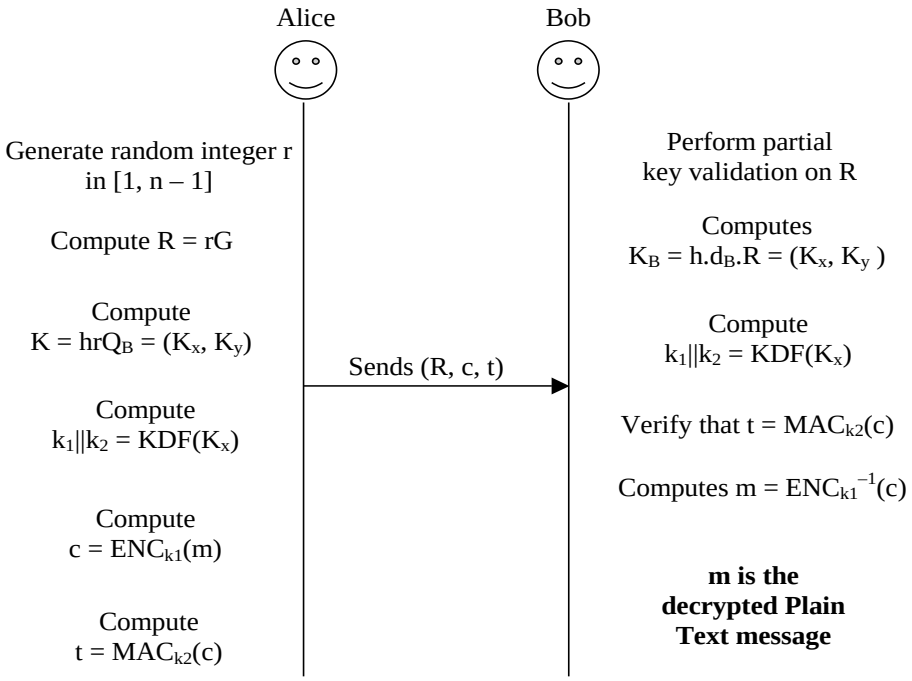


Figure 1: Elliptic Curve Authentication Encryption SchemeIllustration

In encryption the Alice encodes a message value to a point, (PM), on the ECAES, then Alice encrypts this message point (PM), to obtain the corresponding cipher text (PC), lying on the same ECAES using the following equation:

PC = [PM+ SK].

Bob subtracts the shared key (SK) from the cipher point to decrypt a receiving cipher text(PC) (PC) to derives the encoded message point (PM), to pursue this equation

PM = [PC-SK]

The additive inverse of (SK), a point (x, y) on the ECAES is another point on the same ECAES (x, p-y) and the same additive inverse is denoted by (-SK).Bob decodes or maps the message point (PM), into the corresponding value, enryption and decryption steps are performed over the points on the given ECAES.

Imperialist Competitive Algorithm

Imperialism is the procedure of spreading the control of an imperial beyond its own limits in a cluster. An imperialist manage the network by direct rule or by less control of arcade to divided cluster using adequate energy. This algorithm is used to find the adequate energy of wireless sensor network to detect in efficient way for using this algorithm. To divide the cluster into sub cluster by using Imperialist Competitive Algorithm(ICA) is one of the most powerful algorithms; it has been used extensively to solve different kinds of optimization problems.

Each group of the node is called a sub cluster; some of the sub cluster in the nodes is selected to be the imperialist. The node has encountered the selected neighboring to the task, the node has better range and algorithm has efficiently utilized the clusters. All the networks of initial node are divided among the imperialists based on their function for instance and choosing cluster head having adequate energy remaining sub cluster nodes are cluster child. The Network in each of domain starts moving toward their relevant position and in the new one,modify the place. The control of each sub cluster is made up of imperialist networks andfunction requires. Imperialist competitive algorithm is based on cluster control. The cluster which is weaker than the others, misses its networks until there will be no network in that. This action is weakest cluster destruction, its imperialist is considered as the best Network. The imperialist Challengeslevel is when there is only one domain is the optimum point.ICA can provide more accurate solutions in less computational time when compared to the coverage, energy-efficient control algorithm and improved the cluster energy.

Attribute partitioning:

Slicing is an efficient method to handle high-dimensional data. Thismethod diminishes the dimensionality of the data by partitioning the attributes into columns. It enables the slicing to handle high dimensional data. So highly correlated attributes are in the same column and the uncorrelated items are redundant. The highly correlated attributes are preserved so as to preserve the correlation among the

attributes for high usefulnessof data.To evaluate correlations between two continuous attributes, where mean-square contingency coefficient is

$$\Phi 2(A1,A2) = [1/\min\{d1,d2\}-1] \sum_{i=1} d1 \sum_{j=1} d2 \{(fij - (fi,fj))^2/(fi,fj)\} \quad (1)$$

Attribute Clustering:

After the computation of attributescorrelations of each pair, clustering is used to partition the attributes into columns. Based on correlation coefficient of attribute, after finding the correlation along with attributes, it is unlike from clustering,, the vertical partitioning is done and the clustering can be applied based on the attribute selection of a database.

Step 1: To estimate the relationship between two continuous attributes first to define correlation coefficient.

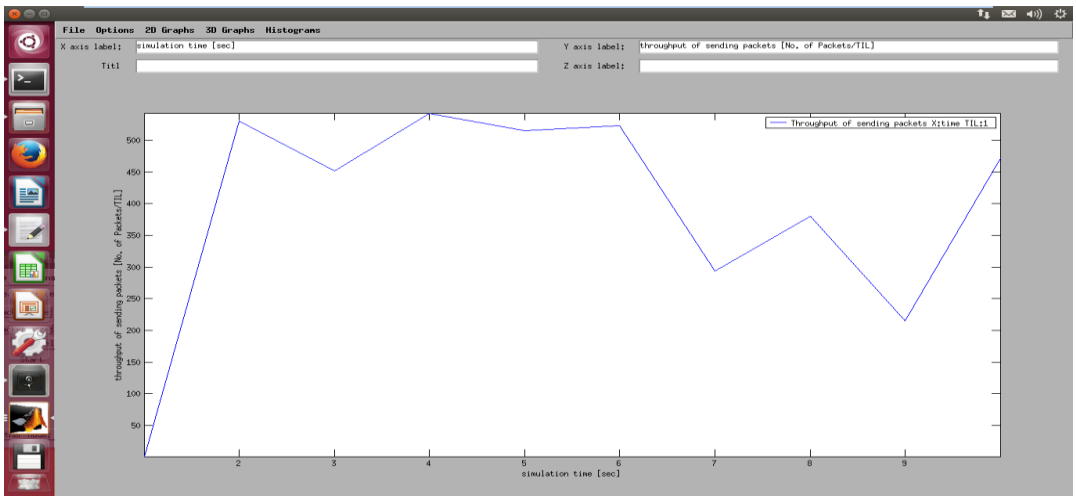
Step 2: Horizontal partitioning can be applied.

Step 3: Attribute clustering for vertical partitioning is based on attribute correlation coefficient to evaluate correlations between the each attribute and, the identifier is defined below:

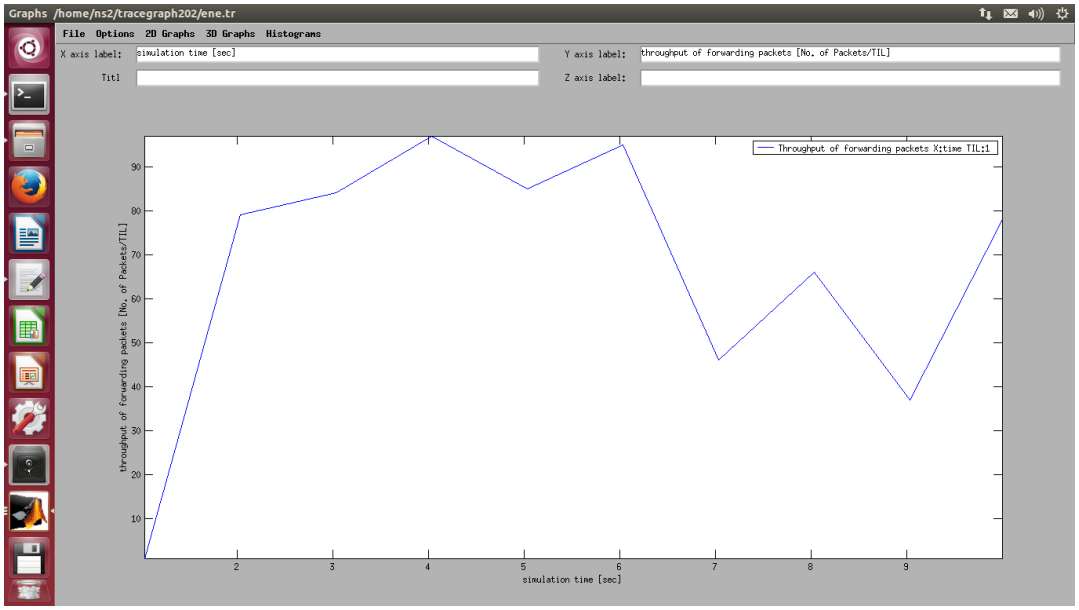
$$d(A1,A2) = 1 - \phi^2(A1,A2) \quad (2)$$

Result Analysis

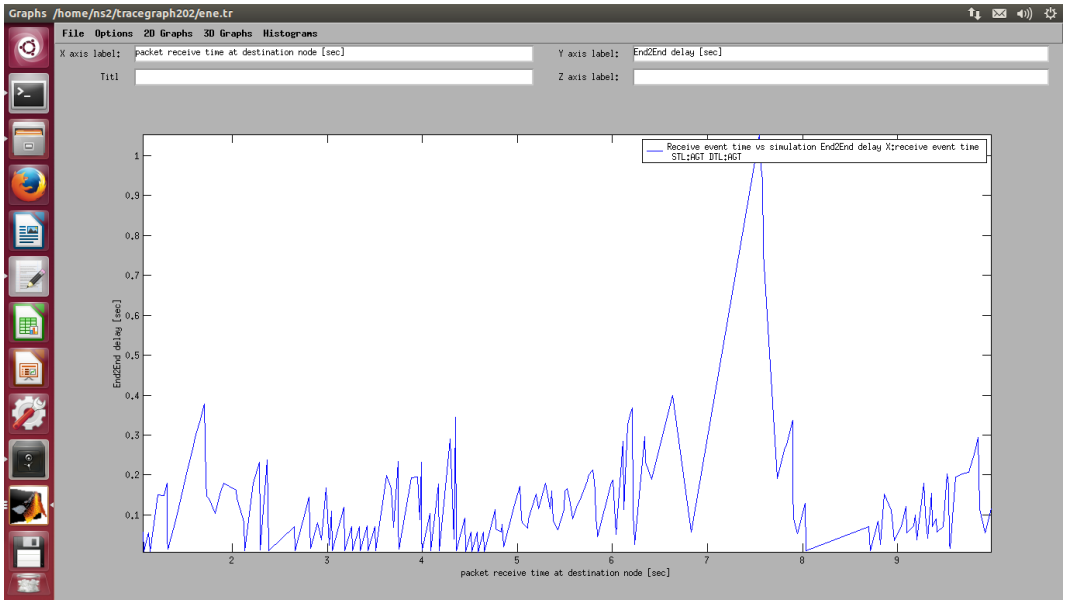
Throughput of Sending Packet



Forwarding Packet Throughput



Throughput of Receiving Packet



Conclusion

In this paper identify the problem is packet dropping and modification to overcome this proposed the ECAES and Imperialist Competitive Algorithm for efficient transmission of data. To prevent the traffic and range within the communication area for identities in sender to receiver for transfer the data without affecting the false

identifiersby using attackers of fake agent. We can partition the cluster into sub-cluster after that to select the cluster head by using imperialist competitive algorithm. Subsequent to selecting the cluster to select the key by using the ECAES algorithm from sender to receiver any fake identifiers is present to avoid using the fake agent attackers.

References

[1] Kennedy Edemacu1, Martin Euku2and Richard Ssekibuule, "Packet Drop Attack Detection Techniques in Wireless Ad hoc Networks" International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.5, September 2014

[2] Tao Shu and Marwan Krunz, Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks" IEEE Transactions on Mobile Computing 2013 EURASIP Journal on Wireless Communications and Networking 2014, 2014:92 Page 2 of 10

[3] Gaurav Bhatia1 and Vivek Kumar, "CTCP: A Cross-layer Information based TCP for MANET" International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.5, No.1, February 2014

[4] Pooja Singh, VikasPareek and Anil K Ahlawat, "Performance Comparison of Energy Efficient Protocols for Wireless Sensor Networks" International Journal of Computer Applications (0975 – 8887) Volume 90 – No 4, March 2014

[5] Shuchi Sharma, Mansi Gupta and Anand Nayyar, "Combating Congestion Problem in Wireless Sensor Network using Combined Dominating Set Technique" International Journal of Advance Research in Computer Science and Management Studies Volume 2, Issue 8, August 2014

[6] Samita Indurkar , N. P. Kulkarni, "Congestion Control in Wireless Sensor Networks" Int. Journal of Engineering Research and Applications www.ijera.com ISSN:2248-9622, Vol. 4, Issue 11(Version - 6), November 2014, pp.109-113

[7] Er. Gurjot Singh and Er. Sandeep Kaur Dhanda, "Quality of Service Enhancement of Wireless Sensor Network Using Symmetric Key Cryptographic Schemes" I.J. Information Technology and Computer Science, 2014, 08, 32-42

[8] Zhidan Liu∗† Zhenjiang Li† Mo Li† Wei Xing and Dongming Lu, "Path Reconstruction in Dynamic Wireless Sensor Networks Using Compressive Sensing" Philadelphia, PA, USA. 2014 ACM

[9] Yamuna Devi C R, S H Manjula, K R Venugopal, L M Patnaik, "Multi-hop Route Discovery Using Opportunistic Routing for Wireless Sensor

Networks" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-12, May 2014

[10] Shuchi Sharma and Anand Nayyar, "Mint-Route to Avoid Congestion in Wireless Sensor Network" Volume 3, Issue 2, March April 2014